Rapid Mission Assurance Assessment via
Sociotechnical Modeling and Simulation

Michael J. Lanham

CMU-ISR-15-XXX

XXXX 2015

School of Computer Science
Institute of Software Research
Carnegie Mellon University
Pittsburgh, PA

Thesis Committee

Kathleen M. Carley Chair
Virgil D. Gligor
Jürgen Pfeffer
Robert Elder
John Graham

Submitted in partial fulfillment of the requirements
for the Degree of Doctor of Philosophy

Copyright © Michael J. Lanham
Keywords: Mission Assurance, Resilience, Assessment, Cyberspace Operations, Cyber, Organization Resilience, Rapid Modeling, Agent Based Model, ABM, Simulation, Modeling and Simulation
Dedicated to my wife, my children, and my country
Acknowledgements

It has been my great fortune to work with and for an outstanding dissertation committee in Kathleen M. Carley, Virgil D. Gligor, Jürgen Pfeffer, Robert Elder (Lieutenant General, US Air Force, Retired) and John Graham (Colonel, US Army). I am particularly indebted to Kathleen for her willingness to take on yet another Army officer, constrained to a very challenging Army time line. I have insufficient words or eloquence to thank everyone adequately, as I know my wife, my children, my family and my friends have missed me these last years.

Throughout this latest journey and on the paths to it, so many people have helped me in more ways than I can enumerate. I have been incredibly fortunate to have so many good people touch my life! Nevertheless, I offer my thanks to the supporting staff, administrators, and developers in the Center for Computational Analysis of Social and Organizational Systems (CASOS). I also offer special thanks to Geoffrey P. Morgan for all the many hours of brain storming, selfless assistance, rapid prototyping, tool development, conducting analysis, and being a friend! Many thanks also to Kenneth ‘Kenny’ Joseph for the hours he spent in developing, configuring, and debugging Construct, helping me do the same. To Peter Landwehr, Wei Wei, and my other fellow doctoral seeking peers in CASOS, I offer my thanks!

The support I have received from the leadership and faculty at the United States Military Academy (EECS) Department of Electrical Engineering and Computer Science (D/EECS) has also been superb. The energy and effort they have contributed to me finishing this trek continues to humble me and generate my gratitude. From covering teaching and grading duties, simple words of encouragement, and forcing me to simply close my door to get work done, my friends and colleagues have been extremely helpful. Thank you also to Dr. Chris Okasaki, for his particular gift to me in being a volunteer editor of this written work. All errors in this text are despite his efforts at helping me be a clearer writer.
Abstract

How do organizations rapidly assess command-level effects of cyber attacks? Leaders need a way of assuring themselves that their organization, people, and information technology (IT) can continue their missions in a contested cyber environment. To do this, leaders should: 1) require analytical and empirical assessments that incorporate organizational and individual cognitive complexities; 2) demand the ability to rapidly model their organizations; 3) identify their organization’s structural vulnerabilities; and 4) have the ability to forecast mission assurance scenarios. Using text mining to build agent based dynamic network models, I examine impacts of contested cyber environments on three common focus areas of information assurance—confidentiality, integrity, and availability. I find that most attacks are in the nuisance range and that only multipronged or severe attacks cause meaningful failure. I also find that organizations can design for resiliency and provide guidelines in how to do so.
# Table of Contents

Acknowledgements ............................................................................................................ iv
Abstract ............................................................................................................................... v
Introduction ......................................................................................................................... 1
  Thesis Statement ............................................................................................................. 1
  Scope ............................................................................................................................... 2
  Definitions....................................................................................................................... 4
  Why is this important? .................................................................................................... 7
  What will this dissertation do?........................................................................................ 9

Literature Review.............................................................................................................. 10
  Introduction................................................................................................................... 10
  Related Areas of Research ............................................................................................ 15
  Related literature corpus and assessment ...................................................................... 31
  Gaps in research into organizational resilience in contested cyber environments...... 66

Data and Models ............................................................................................................... 69
  Introduction................................................................................................................... 69
  Organization—a working definition ............................................................................. 70
  Organizations’ Self-Documentation ............................................................................. 71
  The Data to Model (D2M) Process—an Overview ...................................................... 72
  Two D2M generated DoD organizational models ........................................................ 75
  Changes to empirical models in support of Agent Based Modeling ............................. 113
  Summary ..................................................................................................................... 113

Network Analytics and Resilience .................................................................................. 114
  Resilience in what context? ........................................................................................ 115
  Static resilience indicators .......................................................................................... 116
  Metanetwork resilience indicators .............................................................................. 118
  New and adjusted metanetwork resilience indicators ................................................. 119
  Resilience indicators for strategic and operational models ......................................... 128
  Entropic and Targeted Attacks .................................................................................... 145
  Conclusion .................................................................................................................. 160

Agent Based Models and Modeling ................................................................................ 162
  ABMs and sociotechnical systems.............................................................................. 163
  ABMs and cyber security research ............................................................................. 164
  Overview of Construct ................................................................................................ 165
  Augmentation of D2M generated and stylized models ............................................... 168
  Experimental Setup ..................................................................................................... 184

Simulations ..................................................................................................................... 189
  Changes to Construct ................................................................................................. 189
  Baseline Analysis ........................................................................................................ 192
  Mitigations .................................................................................................................. 195
  General results ............................................................................................................ 195
  Specific results ............................................................................................................. 195

Heuristics ........................................................................................................................ 199

Limitations and Future Work .......................................................................................... 204

Text-mining as basis of organizational modeling.......................................................... 204
Introduction

How do organizations assess command-level effects of cyber attacks? Leaders need a way of assuring themselves that their organization, people, and information technology (IT) can continue the organizational missions in a contested cyber environment. To do this, leaders should: 1) require assessments be more than analogical, anecdotal or simplistic snapshots in time; 2) demand the ability to rapidly model their organizations; 3) identify their organization’s structural vulnerabilities; and 4) have the ability to forecast mission assurance scenarios.

Thesis Statement

Organizations can design themselves to improve their organizational resilience in contested cyber environments. They can do this by deliberately adjusting their formal and informal structures (human and IT) to reduce their susceptibility to events in contested cyber environments. They can also assess the improvements in resilience to contested cyber environments due to the chosen structural and functional mitigations and fold the assessed shortfalls into a continuous improvement cycle. The fundamental expectation is that organizations can indeed design their structures and their functions to be resilient to contested cyber environments. Consequences of such efforts include organizations projecting and achieving higher levels of mission assurance than they might otherwise.

Using a rapid data to modeling approach, this research shows that organizations can develop complex network-based models of characteristics that impact the ability of the organization to continue its mission(s). These models are multimodal in that there are multiple node types and multiplex in that there can be multiple links between nodes of the same types as well as links between nodes of different types. Node types include people, IT systems, resources, IT resource, tasks, knowledge, roles, and beliefs. The models are compatible with analysis techniques from graph theory and social network analysis (SNA) research. The models also support over time analysis, also called dynamic network analysis (DNA). These analytic techniques support objective analysis across multiple dimensions as well as various levels of aggregation or disaggregation of nodes and links. The rapidity and flexibility of these network-based models lend themselves to rapid self-assessments,
especially when compared to more traditional cyber and general-purpose risk assessment frameworks’ data gathering and analysis techniques.

This research and dissertation shows it is feasible and appropriate to convert these multidimensional models to inputs for multiagent simulation environments. The outputs of the simulations support assessments of organizations in nominal and degraded cyber environments. Simulating effects of contested cyber environments (i.e., loss of confidentiality, loss of integrity, and loss of availability), the work shows that structural mitigations (i.e., modifications of the quantity and frequency of human-to-human links) as well as modifications to various IT dependencies (i.e., modifications of the quantity of IT systems and rapidity of replacements being brought into the system) are feasible and effective at reducing the impacts of contested cyber environments. With efficacious mitigations, organizations and leaders can increase their confidence of mission assurance in contested cyber environments.

Scope

There are multitudes of ways to scope a dissertation in this research area. The following, combined with the definitions in Appendix 1 (page 230), delineate the boundaries of the problem space for both practical and tractability reasons.

The analyses for the various organizations under test focus on the formal decision makers of the organization—that is they are command-level analyses. However, decision makers do not operate in a vacuum; they have surrounding and supporting structures that both inform and constrain decisions and actions. I account for these structures by modeling them as fellow organization members, fellow decision makers, and IT systems. I also include IT resources and non-IT resources, organizational and groups’ tasks as well as representations of organizational and individual knowledge. I constrain the analyses to short-term (e.g., hours to days) measures of performance (MoP) and measures of effectiveness (MoE) to compare and contrast conditions under test. I treat modeling and analyses of long-term impacts (e.g., weeks to months) as out of scope while acknowledging such work would be very interesting.
The research uses stylized adversaries capable of creating effects in and through the IT systems and IT resources of the modeled organizations. The dissertation also scopes the effects of contested cyber environments (see also Definitions) to three (3) of the five (5) categories in the Committee of National Security Systems (CNSS) Information Assurance (IA) ontology: Confidentiality, Integrity, and Availability. These adversaries, discussed in detail later, are neither omniscient nor omnipotent. The dissertation does not incorporate the remaining two (2) CNSS IA categories of authentication or nonrepudiation.

Modeled adversaries create availability effects against random or specific IT systems within the modeled organizations with varying probabilities of effect. Modeled adversaries can also create availability effects against various technology supported communications mediums in the model (e.g., telephone, classified and unclassified email). The models do not mimic the technical mechanisms an adversary could use to create these effects. The results for the modeled organizations range from no measurable effects to effects high enough to generate noncatastrophic results. It was not part of the research plan to generate the degenerate case of 100% loss of all communications technology and/or IT systems within an organization.

There is also a set of stylized integrity agents that act, at the various levels of security within the organization models, as spreaders of disinformation. These are abstracted attack vectors without specific implementation techniques in the model. The results from the modeled organizations indicate that various structural configurations speed and slow the spread of disinformation. There are also distinct differences in the longevity of disinformation in decision making circles compared to the organization as a whole.

Finally, I have modeled a passive confidentiality agent as an information sink on the unclassified security level of the models. The intention is to begin the process of understanding how to model confidentiality leaks—though I will not be ascribing specific operational impacts to those leaks (e.g., the impacts of intellectual property leaking to a competitor firm or the designs for modern military equipment).

The short duration cyber environments represent a first step in a long term research plan. It is easy to foresee extensions to this work that would incorporate longer lasting contested environments to trigger and assess more pronounced adaptive and maladaptive
behaviors. It is also easy to foresee extensions where attacks incorporate series effects (e.g., attack, pause, attack) as part of a deliberate effort of adversaries to generate adverse environments for organizations under study.

**Definitions**

Short, plain English definitions are used in this portion of the dissertation with more detailed and thorough definitions in Appendix 1.

What is a *contested cyberspace* (*cyber* for short) *environment* and why does it matter? Quite simply, a contested cyber environment is a human-built complex system. It includes interconnected telecommunications and information technology networks and network-enabled devices. Most importantly the technology intertwines with people and man-made and natural processes that can, and do, interfere with the designed and intended purpose of the environments. I’ll address the ‘why it matters’ portion of the opening sentence shortly.

The United States Air Force (USAF) developed a nondoctrinal definition of *mission assurance* that means the USAF and its units can “fight through an attack” (Elder, 2008; Webber, 2010) (see also the definition of Mission Assurance on page 231). Importantly, the decision makers that developed this approach were not information security (INFOSEC) or computer security (COMPUSEC) practitioners but were operations generalists. Those generalists, by long experience and exposure, have learned the complex choreography of the USAF’s many missions has a central core: successful execution of military operations. The situation is akin to organizations (e.g., oil exploration) that have multiple subordinate elements (e.g., Human Resource (HR), Finance, Logistics) that perform necessary, even critical functions, that remain, fundamentally, not the primary raison d’être of the organization. This USAF concept of mission assurance gives its leadership confidence that it can perform its core and essential supporting missions in the face of adverse circumstances. The confidence is predicated on the expectation of future events. This expectation aligns with the right side of Figure 1 labeled “Event Management” that illustrates risk reduction with operating through adversity.

**Figure 1** depicts mission assurance as an abstract aggregation of two major components: (1) Iterative application of one or more risk management frameworks; (2) event management. It is important to note that in event management has at least three components:
(1) Pre-event rehearsal(s); (2) adaptation during and possibly after the event; and (3) post-event recovery. In the figure, I have also made explicit the need to record and learn from the preceding events—deliberately choosing to not learn lessons qualifies as a maladaptive practice that is beyond the scope of this work.

This continued functioning in the face of adversity leads us to our next, related definition. One way of assessing mission assurance is by leveraging the concept of resilience. According to Merriam-Webster’s dictionary, resilience is “an ability to recover from or adjust to misfortune or change” (resilience, 2012). This dissertation applies the definition in two ways: one through a new mathematical definition as a function of congruence between an organization’s requirements, needs, and redundancies; the second, applied to multiple measures of interest, is the time to return to equilibrium after disruption.

A visualization of the disruption of this new metric, and various other measures of interest is shown in Figure 2 (see also the more complete discussion in the Network Analytics and Resilience chapter starting on page 114). There are pre-event measures, one or more events, post-event degradation of the chosen measures, and recovery in some fashion.
Implicit in this figure is there is a pre-event equilibrium, and there is survival—resilience for stochastic measures cannot exist nor can it have a definition in the absence of survivability.

![Figure 2 Dynamic visualization of resilience for an arbitrary measure of interest (MoI) (Morgan & Lanham, 2012)](image)

The just discussed motivator of “contested cyber environments” scopes the dissertation to the type of adversity, as does focusing on organizational resilience. Of the multiple ways to model and simulate a contested cyber environment, I simulate abstract mechanisms instead of specific re-creations of named adversaries, technical activities or specific implementations of what the Department of Defense (DoD) defines as computer network attack (CNA) (Joint Staff J7, 2010a).

*Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy [emphasis added] information resident in computers and computer networks, or the computers and networks themselves.*

The Committee of National Security Systems (CNSS) definition of information assurance helps in this decision by creating an ontology with five (5) effects labeled confidentiality, integrity, availability, authentication, and nonrepudiation (CIAAN) (2010). I use abstracted mechanisms that create one or more of the first three effects (i.e., CIA) based on an assessment that negative effects that start in the authentication and nonrepudiation categories often serve as waypoints en route to deliberate effects within the first three categories. When combined together, the use of abstract mechanisms and the CIA ontology supports rapid modeling of effects rather than the specific technical modeling of SYN flood
denial of service (DoS), distributed DoS (DDoS), cryptographic or message replay attacks, or other specific forms of CNA.

**Why is this important?**

Since the birth of the integrated chip, there has been an incredible growth in the ways humanity has put IT to use. Though there are still elements of humanity that remain largely untouched by electricity as well as information technology, it’s the electricity and IT using organizations that interest us in this research. The growth of the penetration of IT in everyday lives should be fairly noncontroversial, with Figure 3 (page 11) through Figure 7 (page 13), depicting examples of growth in civilian and military use of information technology. With the growth in use, there is an accompanying rise in risk that disruption of IT can negatively affect the people and organizations accustomed to its presence.

Returning to the two parts of mission assurance in Figure 1, leaders plan and work to reduce their organizations’ various risks as well as plan their reactions to misfortune and adversity. In virtually every risk management framework, a recurring task for organizational leaders is assessing and adjusting framework compliance and adherence measures. Such activities however are beyond the scope of this research effort.

Missing in many of risk management frameworks however are explicit acknowledgements and deliberate planning and rehearsal for the actual occurrence of risk events. Deliberate planning and rehearsal is an implicit acknowledgement of non-zero risk, and a solid foundation for leaders and subordinates alike to increase confidence in mission assurance. Incorporating lessons learned from previous assessments and events is also salutary to increasing perceptions of mission assurance. Short of rehearsing for or living through adverse events, there are other tools available for organizations to increase their perception of mission assurance—specifically socio-technical simulations that support forecasting efficacy of planned mitigations and reactions.

Another shortfall in many risk management frameworks is the oft-repeated phrase that the assessments are snapshots in time. This shortfall becomes problematic when reflections of the organization from weeks, months or years ago conflict with leaders’ perceptions of *now*. Rapidly constructed socio-technical simulation models help reduce the
gap between perceptions of now and snapshots of the past, as well as speed contingency planning.

With increased use of IT, leaders of organizations (Loveland & Lobel, 2012), as well as national and military leaders (Lynn, 2010), have assessed there are increased risks to their organizations’ ability to adequately perform missions in contested cyber environments. The President of the United States issued Homeland Security Presidential Directive 7 (HSPD-7) that specified 31 policies the executive branch would pursue to protect assets from all manner of threats—including cyber threats (2003). For all of these leaders, human adversaries are not the only concern with respect to their reliance on cyberspace capabilities. Natural phenomena can also inflict the effects of a contested cyber environment—a degradation, denial, disruption, or destruction of cyber/IT assets. Hurricane Katrina (Piper & Ramos, 2006) and Super Storm Sandy (Carew, 2012) degraded communications for consumers, emergency services, and governmental entities quite extensively. Undersea events from earthquakes to dragging anchors can break undersea fiber optic cables—inflicting both total and partial loss of availability (Niccolai, 2008; Rotenburg, Schneier, McConnell, Zittrain, & Donvan, 2010). Man-made threats to cables include advanced submarines and technology that support eavesdropping (Sherry, Drew, & Drew, 1998; The Associated Press, 2005) to vandalism or sabotage (Reardon, 2009; Shin & Garske, 2012) that can inflict losses of confidentiality and availability on those who use the undersea cables.

Organizations with missions enabled by, or outright reliant on cyber resources, face some amount of risk that the organizations could fail at those missions in a contested cyber environment. IT-enabled supply chain dependent organizations can suffer sufficient degradation or disruption that they are unable to continue their manufacturing, selling, or other missions and may cease to operate (Min & Zhou, 2002; G. E. Smith, Watson, Baker, & Pokorski Ii, 2007). Organizations that are less reliant on IT for their primary day-to-day operations may find that they are less able to conduct other forms of business or operations as well as their secondary functions (e.g., accounts receivable, accounts payable, shipping and receiving, and timely resupply to subordinates, peers, or customers) during periods of contested cyber environments. IT-reliant organizations such as electronically traded funds (ETF) may also cease to operate, cease to exist due to monetary losses, or otherwise suffer such degradation they cannot sustain their business model—though these types of
organizations are beyond the scope of this work. Targeted attacks against network-enabled supervisory control and data acquisition (SCADA) can affect organizations that use SCADA such as electric power companies. Degraded SCADA systems could potentially trigger cascading failures such as the 2003 electrical black out in portions of the U.S. and Canada (U.S.-Canada Power System Outage Task Force, 2004). The risks of cascading failure rise with increased interconnections between organizations when those interconnections lack physical and procedural safeguards.

The proceeding paragraphs of this section, in abbreviated form, make the case that the effects of a contested cyber environment can be adverse to organizations’ ability to perform their missions or business operations. Such outcomes are contrary to fundamental business interests, and for militaries could hinder the ability to defend or assert national interests. Given that risks of contested cyber environments are unlikely to be zero, there is a prima facie case that leaders should be confident in their organizations’ ability to adapt and operate despite such environments.

What will this dissertation do?

There are three broad sets of deliverables within this dissertation, listed in Table 1. The first is an approach for rapidly assessing organizational resilience to contested cyber environments. The second is a theory of command-level resilience to those environments. The third is a reusable, empirically grounded agent based dynamic network model and associated methodologies for assessing the command-level resilience to cyber attacks and events.

Table 1: Three primary sets of deliverables

<table>
<thead>
<tr>
<th>Develop an approach for assessing organizational resilience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a command-level theory of resilience to contested cyber environments</td>
</tr>
<tr>
<td>Develop a reusable, empirically grounded agent based dynamic network model and associated methodology for assessing command-level resiliency to cyber attacks &amp; events</td>
</tr>
</tbody>
</table>
Literature Review

Introduction

Mission assurance, having a level of confidence in the resilience of an organization, its ability to recover from or adjust to cyber events, along one or more measurable dimensions is necessarily a multi-disciplinary effort. This literature review expanded from those topics depicted in Figure 1 to include areas of interest as diverse as emergency management, high reliability organizations (HRO), organizational behavior and learning, supply chain management (SCM), cyber security, modeling and simulation (M&S), SNA and network science. Each of these research areas have information and results that can shed light onto each other’s areas of interest as well as this dissertation. The review also incorporates research from cyber specific risk management.

The review offers an introduction to the increasing importance that IT and cyber capabilities has in American’s lives. The Related Areas of Research section presents a high level summary of several related fields of research that touch on but do not directly address organizational resilience to contested cyber environments. The Related literature corpus and assessment section discusses my bibliometric approach to assessing a selected corpus of citations. The Gaps in research into organizational resilience in contested cyber environments section illustrates the gaps in the literature regarding organizational resilience especially to contested cyber environments as well as need to improve the application of M&S to help cross the gaps. The review will reinforce the links between the research areas that the authors within the corpus identified as well as illustrate the need for more links between research areas that share common areas of interest without normally overlapping.

Increasing use of Information Technology (IT) in many civilian industries and organizations

Since the creation of the integrated circuit, there has been an incredible growth in the ways humanity has put IT to use. Though there are still elements of humanity that remain largely untouched by electricity as well as the information technology, it’s the electricity and IT using portion that interests us in this literature review. Two indirect indicators of the growing use of IT within civilian infrastructures are the growing demand and use of the radio frequency spectrum as well as the sales of computer and IT related equipment over the last
35 years. Figure 3 depicts the frequency allocation by the Federal Communications Commission (FCC) in 2012 with Figure 4 providing the contrast in growth of frequency-use demands. The growth in demand for the various uses of frequencies is a reflection of the growth in the number of ways humanity has put IT to use in our industries and our daily lives.

Figure 3: Federal Communications Commission (FCC) Frequency Allocation Chart circa 2003 (US Department of Commerce, 2003)

Figure 4: FCC Frequency Allocations circa 1975 (Elder, 2008)

A second indicator, and there are too many possible indicators to enumerate even a tiny fraction, is the sales growth of computers from their inception with ENIAC in 1946 (Weik, 1961) to 2012. There is an apocryphal story that IBM’s Tom Watson, Jr., opined he foresaw a market for about 5 mainframe computers in the world in the 1950s\(^1\), while Gartner forecasted over 400 million computers shipping around the world in 2012. Figure 5 reflects sales growth for personal and desktop computers, with Figure 6 depicting the growth of

\(^1\) IBM asserts this story is a misunderstanding of statements made by Tom Watson, Jr., in their Frequently Asked Questions (FAQ) (IBM, 2007)
super-computers—the nearest analog to Watson’s mainframes that was IBM’s core business through the 1980s. The figure is depicting the distribution of super-computers across the continents of the globe, and limited to the top 500 super computer systems—the entry level has moved up to 76.5 teraflop (Tflop)/s (floating point operations per second) from 60.8 Tflop/s in May 2012 (Meuer, Strohmaier, Simon, & Dongarra, 2012)

**Figure 5:** Sales growth for personal computers from 1998 to 2011 (Arthur, 2011)

**Figure 6** Growth in installed super-computers by continent since 1994 (Meuer, Strohmaier, Dongarra, & Simon, 2012)

**Increasing use of IT by US Department of Defense (DoD)**

The DoD’s growing division of the frequency spectrum also reflects this growth in frequency requirements. US military forces are, in some respects, the most IT-enabled military on the planet with their blue-force-trackers, remotely piloted aircraft (e.g. Predators,
Global Hawks), small unit access to real-time streaming video of their area of operations, as well as line of sight (LOS) and beyond line of sight (BLOS) encrypted radios. Such is the extent of infiltration of IT, that the White House situation room had as-it-happened information sent around the globe from Pakistan during the raid to kill Osama bin Laden (Souza, 2011). Figure 7 is a DoD specific chart depicting the use of the radio frequency (RF) spectrum that, while not all-inclusive, is a reflection of the number of uses for the RF spectrum that simply did not exist 35 years ago (e.g., Global Positioning System (GPS), Unmanned Aerial Vehicles (UAVs), Defense Satellite Communications System (DSCS), and Mobile Subscriber Equipment (MSE)).

Figure 7 US DoD Frequency Allocation Chart circa 2010 (Defense Business Board, 2010)

**Increasing risks from contested cyber environment**

With increased use of IT, leaders of organizations (Loveland & Lobel, 2012), as well as national and military leaders, are assessing there are increased risks to their ability to execute their missions despite contested cyber environments. Former Deputy Secretary of Defense William J. Lynn III, among many others, has published his belief that the very advantages IT systems give the US, potentially allow adversaries of all kinds anti-US operational opportunities. Those opportunities can range from disrupting US logistics support
to operations around the globe as well as degrading the perception of control of globally deployed forces by national leaders (Lynn, 2010). The President of the United States (POTUS), also growing concerned about the perceptions of risks to ‘critical infrastructure,’ issued Homeland Security Directive 7 (HSPD 7) that enumerated 31 policy positions that the executive branch would pursue with respect to protecting assets from all manner of threats—including cyber threats (Office of the President of the United States, 2003).

Human adversaries are not the only concern for the national leaders around the globe. Natural phenomena can also inflict the effects of a contested cyber environment—a degradation, denial, disruption, or destruction of cyber/IT assets. Hurricane Katrina (Piper & Ramos, 2006) and Super Storm Sandy (Carew, 2012) degraded consumers’ communications quite extensively, as well as emergency services’ and governmental entities’. Undersea events can also break segments of the global undersea fiber optic cable network—inflicting a loss of availability (Niccolai, 2008; Rotenburg et al., 2010). Man-made threats to undersea cables also include advanced submarines and technology that support eavesdropping on those same cables (Sherry et al., 1998; The Associated Press, 2005)—inflicting a loss of confidentiality. Having leaders that are aware of possible cyberspace related risks is a necessary condition for organizations to take steps to reduce those risks as well as take steps to ensure their ability to operate despite any contestation of their cyber environments.

**Contested cyber environments as risks to organizational resilience**

Emergency services, HROs, governmental leaders and their staffs are not the only stakeholders contested cyber environments put at risk. Organizations with missions enabled by, or completely reliant on cyber resources, face some amount of risk that the organizations could fail at those missions in a contested cyber environment. Organizational dependency on IT can vary anywhere along the spectrum from no dependency at all to the opposite end where the organization will cease to meaningfully operate without IT.

Organizations that are less reliant on IT for their primary day-to-day operations may face degradation in their abilities to conduct other forms of business, operational, or secondary functions (e.g., accounts receivable, accounts payable, shipping and receiving, timely resupply to subordinates, peers, customers) during periods of contested cyber environments. Organizations dependent on supply chains could suffer sufficient degradation
or disruption that they are unable to continue their manufacturing, selling, or other missions and may cease to operate (Min & Zhou, 2002; G. E. Smith et al., 2007) if the disruption lasts too long. Organizations and business that are, at heart, IT reliant may also cease to operate, cease to exist due to losses, or otherwise suffer such degradation they cannot sustain their business model; electronically traded funds (ETF) companies can often define exactly how much money they lose during service interruptions and work hard to minimize those potential losses.

Organizations that provide, operate, and maintain the many parts of national critical infrastructure also have some vulnerability to contested cyber attacks through their use of in-band and out-of-band control systems (often called Supervisory and Control Systems (SCADA)). Those and other organizations can also have indirect at risk outside their direct control. Cascading failures of power systems, such as the 2003 electrical black out in portions of the US and Canada (U.S.-Canada Power System Outage Task Force, 2004) represent a class of indirect risk. Where interconnections between providers of any cyber related service exists, degradation or disruption of one or more providers may, like electrical distribution systems, cause a shifting of load to other elements of cyberspace—those elements may or may not be capable of supporting the new demands.

Related Areas of Research

What does resilience mean?

What is resilience? Revisiting Merriam-Webster, it is “an ability to recover from or adjust to misfortune or change” (resilience, 2012). There are variations on this definition that scope the definition to ecology and life sciences fields. The physics community has a definition of resilience as the potential energy stored in an elastic material when the material is deformed (resilience, 2003). When applied to technical systems, and in particular systems of systems, some definitions add language that requires recovery be to the level of performance or measure of interest present prior to the event (Bishop, Carvalho, Ford, & Mayron, 2011). Other definitions require the system(s) of interest be able to predict disruption (Pflanz & Levis, 2012), and that the system will function as the owners ‘required and intended’ (Horning, 2009) despite being in a hostile environment.
Still others perceive resilience as a series of traits (Coutu, 2002) that companies and assessments must then operationalize by converting the traits to measures of performance (MoP) and measures of effectiveness (MoE). Gunderson asserts that resilience, is effectively “magnitude of disturbance that can be absorbed before the system redefines its structure by changing the variables and processes that control behavior” and refers to Walker et al calling this “ecological resilience” (Gunderson, 2003).

**Resilience Engineering**

The variety of definitions, especially applied to systems of humans and equipment has even lead to the establishment of a field of engineering entitled “Resilience Engineering.” Practitioners of resilience engineering view systemic or organizational mishaps as failures to maintain systems, processes, and thought processes as the inverse of adaptability and resilience (Hollnagel, Woods, & Leveson, 2006; Madni & Jackson, 2009a; REA Public Affairs, 2013).

In the resilience engineering domain, the focus tends toward safety as a primary metric. Madni and Jackson collected and synthesized fourteen heuristics in their review of the growth of resilience engineering (2009d) that they break into near-term and longer-term categories: reaction and adaptation respectively (2009a). In a different formulation, Westrum asserted resilience has three meanings: the ability to prevent something bad from happening; the ability to prevent something bad from becoming something worse; and the ability to recover from something bad once it has occurred (2006). Westrum also distinguishes coping by being adaptive (e.g., organizations changing themselves in response to a crisis) and being armored (e.g., a tank) (2006). Both examples reflect different approaches to survivability with one being very hard, and very resistant to minor perturbations. Unfortunately, once disruption reaches the tank-armor’s breaking point, catastrophic failure is the typical, and often unsafe, outcome. This opposite state of resilience has earned the label brittleness (Hollnagel et al., 2006; Madni & Jackson, 2009a).

**Why resilience to contested cyber environments?**

This literature review will limit the scope of reviewed adversity to the effects of contested cyber environments wherever feasible, though there is a surprising paucity of research that restricted itself to IT based adversity or even passingly referred to IT based
adversity. In addition to this dissertation, other researchers have taken note of the dearth of research into cyber effects (Chapman, Leblanc, & Partington, 2011; Leblanc, Partington, Chapman, & Bernier, 2011). Enumerating or creating ontologies of specific origins of threats (e.g., insider/outsider, malicious/nonmalicious, natural/manmade) is certainly a time honored way of problem decomposition for cyber security (Bishop, Engle, Peisert, Whalen, & Gates, 2009a, 2009b; Chapman et al., 2011). Clearly the nature of threat(s), their likelihood, and their ability to incur an effect contribute to organizations decisions about resource allocations and residual risk acceptance. Rather than adding to this well developed, and yet still evolving body of research, this dissertation explores the need for organizations to be resilient to the effects of events in the cyber environment. Organizations and people must be able to adapt to or otherwise cope with the effects to return to some post event equilibrium. Which effects of contested cyber environments in particular? We will co-opt three of the five pillars of information assurance: confidentiality, integrity, availability, authentication, and nonrepudiation.

In some research or operations circles, this focus on the effects of cyber environments could fall under the label of ‘effects based operations’ (EBO) (P. K. Davis, 2006). I will not be exploring this application of the EBO label. Indeed, this focus on effects defers to other...
authors the comprehensive discussions of how contested environments come into being. Readers will not see in this dissertations details and explorations of the manipulation of bits, bytes, protocols, buffers, and other technology-oriented discussions on how to create contested cyber environments nor the efforts to identify appropriate targets to achieve desired objectives.

**Organization adaptation and learning**

Generalized discussions of resilience, the ability of both people and organizations to improvise (a key trait identified by Coutu (2002) and Madni (2009d)) and adapt to adversity are useful for developing perspectives and theoretical frameworks for organizational resilience. Fundamental to the idea of adaptation to adversity is the idea that organizations are capable of learning new behavior in the first place (Gunderson, 2003). It is clear from observation that organizations can learn—lists of companies, and even countries that modify their behavior over time would be long, and filled with varying levels of success from survival through flourishing. The inverse is equally true, the history of humanity is replete with sovereign entities, countries and companies that have ceased to exist—arguably through their inability to adapt to changing conditions.

What motivates or provokes those changes, the adaptation, and learning? There are three longstanding observations of organizational learning, also shown in Table 2. The first observation is organizations base their behavior on routines, on their collective perception of organizational history, and on their goal orientation (Crichton, Ramsay, & Kelly, 2009; B. Levitt & March, 1988). The second observation is behavioral changes occur through positive and negative feedback loops, especially distinctions between perceptions of success and failure, as well as incremental modification of routines (B. Levitt & March, 1988; Norris, Stevens, Pfefferbaum, Wyche, & Pfefferbaum, 2008). The third observation is those organizations’ self-perceptions of being adaptable, of being able to cope with the variations of every day requirements as well as manage unusual circumstances are a key component of making the belief a reality (Dutton & Dukerich, 1991). Knowing the above, the reader may be wondering what then inhibits organizational learning and adaptation?

<table>
<thead>
<tr>
<th>Table 2 Three observations on organizational learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations base their behavior on routines, on their collective perception of organizational history, and on their goal orientation</td>
</tr>
</tbody>
</table>
Behavioral changes occur through positive and negative feedback loops, especially distinctions between perceptions of success and failure, as well as incremental modification of routines.

Organizations’ self-perceptions of being adaptable, of being able to cope with the variations of everyday requirements as well as manage unusual circumstances are a key component of making the belief a reality.

There are at least three structural difficulties in learning from experience identified in research: paucity of experience, redundancy of experience, and complexity of experience (B. Levitt & March, 1988), shown in Table 3 below. Without experience in a degraded environment to establish routines, fail-over plans, and without a perception of “we’ve done this before,” an organization has not learned the true effects of a degraded cyber environment to their particular situations. The situations they could face are each a possible source of creating routines the company switches to in contested cyber environments.

The success versus failure ratio can only change with modifications to its numerator or denominator. Behavioral Psychologists have long known that repetition is a key component of learning for individuals, and repetition is the key to adjusting the organizational perception of success: failure ratios for given scenarios or general sets of circumstances.

The third component of organizational learning, as well as the third challenge set the stage for non-trivial exercises and rehearsals. The natural state of IT-based capabilities for many users is that there is ‘always’ something going amiss with their tools, networks, or other IT-based capabilities. But without shifting from the aperiodic, noncatastrophic, low-duration, nonpervasive outages of ‘normal,’ organization members will face unexpected complexities and potentially lose their own perception of adaptability—they are akin to the Westkin’s armored tank where the energy resistance capacity of the armor is exceeded and catastrophic results occur.

<table>
<thead>
<tr>
<th>Table 3 Structural challenges to organizational learning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paucity of experience</td>
</tr>
<tr>
<td>Redundancy of experience</td>
</tr>
<tr>
<td>Complexity of experience</td>
</tr>
</tbody>
</table>

This perception of adaptability is a point of pride for the various US armed Services—virtually every US Army and US Air Force Posture Statement in the last fifteen years has
specifically called out adaptability, learning or transformation (Office of the Chief of Staff of the U.S. Air Force, 2012; Office of the Chief of Staff, 2012). Each Service also embodied adaptability in the creation of new doctrine in the 1980s (Romjue, 1984) and 1990s.

**Incident and event response and rehearsal**

Many United States Government (USG) documents call for better and more preparedness for using IT and other cyber capabilities to offset declining budgets and resource levels, increase efficiencies, and increase efficacy of available resources. These documents often advocate for the defense and sustainment of existing and future IT based capabilities. What the documents omit, with some recent exceptions such as (Kaminski, Gosler, & Von Thaer, 2013), are directives to leaders to train and practice their missions within degraded environments—what the US military often refers to as specified tasks in contrast to implied tasks. One outcome of this lack of deliberate training in degraded environments is leaders are training for environments with incompetent adversaries while blithely assuming defeat of attacks or rapid restoration of lost assets (Lanham, 2012c). The omission also reinforces all three structural difficulties in learning from experience: paucity of experience, redundancy of experience, and complexity of experience (B. Levitt & March, 1988). Indeed, the dominant tone of many cyber related government documents is fear of the loss of IT and cyber capabilities with few, if any, references to the requiring reasonable preparedness and expected adaptation to the destruction, disruption, or degradation of cyber resource. Without loss of IT or degradation of IT training to construct lessons, the palpable fear by reporters and luminaries in the open press could simply be another example of propagating disaster myth (Norris et al., 2008; Tierney, Bevc, & Kuligowski, 2006)—the sky will fall without our necessary IT.

Though I found no evidence of conscious effort to avoid purposeful and meaningful rehearsal of contested cyber environments, there is considerable effort dedicated within risk management and cybersecurity communities at preventing, or reducing to ‘acceptable levels of risk,’ the occurrence of cyber events. The USG has built an information assurance model of cyber security widely used by the its three branches, academia, and industry.
Information Assurance pillars

There have been long running efforts by USG entities to fortify and protect their IT systems and cyber capabilities, prominent among them were DoD Directive 5200.28 *Security Requirements for Automatic Data Processing (ADP) Systems* of the 1980s, which spawned DoD 5200.28-STD *Department Of Defense Trusted Computer System Evaluation Criteria*, aka “The Orange Book” and its accompanying “Rainbow Series.” Efforts continued through the creation of *Common Criteria* of the 1990s, and DOD Directive 8500.1E *Information Assurance* encapsulates current DoD efforts. The USG has been making additional strides to implementing effective Information Security through the passage and implementation of the Federal Information Security Management Act (FISMA)("FISMA," 2002), which tasked the heads of federal agencies and the National Institute of Standards and Technology (NIST) to standardize INFOSEC risk models in support of legislative oversight responsibilities. A portion of the DoD contribution to NIST’s standard framework, applicable to national security systems, is a glossary of terms provided by the Committee on National Security Systems (CNSS) Instruction *National Information Assurance (AI) Glossary* (CNSS, 2010).

FISMA established three fundamental elements to the notion of information security: integrity, confidentiality, and availability.

CNSS Instruction (CNSSI) No. 4009 goes on to add two additional elements to the definition of information assurance—a rewording of FISMA’s definition of ‘information security.’ CNSSI 4009 defines each of the five pillars of information assurance as shown in Table 4 below (2010). The Department of Defense’s definitions draw from these definitions and sometimes add additional verbiage (Department of Defense, 2007). With these five terms, we can characterize events as diverse as SYN floods or other forms of denial of service attacks to undersea cable breaks as a loss of availability. Replay attacks, injecting false radar tracks into radar systems, and changing the contents of personnel and finance computers all naturally fall under loss of integrity effects. Key logger trojans, universal serial bus (USB) key-capture devices, account credential thefts all fall first under the effect of compromised or lost authentication, with likely follow-up effects in confidentiality, integrity, and nonrepudiation. It is with the first three of these effects that I will focus the dissertation.

<table>
<thead>
<tr>
<th>Term</th>
<th>CNSS Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>confidentiality</td>
<td></td>
</tr>
<tr>
<td>integrity</td>
<td></td>
</tr>
<tr>
<td>availability</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: CNSSI 4009 Definitions of CIAAN
The Five D’s—Disrupt, deny, degrade, destroy, and sometimes deceive

With the DoD, discussions of contested cyber environments frequently revert to the four elements within its definition of computer network attack (CNA)—disrupt, deny, degrade, and destroy—and sometimes adds the element of deceive from the definition of Information Warfare (IW). Literature associated with cyber security and contested cyber environments frequently use these terms, and their definitions are important for further discussions. The DoD’s Joint Publication (JP) 3-13 Information Operations (2006), defined these terms as shown in Table 5. These definitions represent different, but neither mutually exclusive nor orthogonal, ways of characterizing contested cyber environments. A visualization of these two characterizations, and how they could overlap in 2D space, is shown in Figure 8. The links represent one way of mapping each of the 5 D’s into one or more of the CNSS 5 pillars of IA.

Table 5: DoD definitions of the five D’s (2006)

<table>
<thead>
<tr>
<th>Term</th>
<th>DoD Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disrupt</td>
<td>To break or interrupt the flow of information.</td>
</tr>
<tr>
<td>Deny</td>
<td>To prevent the adversary from accessing and using critical information, systems, and services.</td>
</tr>
<tr>
<td>Degrade</td>
<td>To reduce the effectiveness or efficiency of adversary C2 or communications systems, and information collection efforts or means. IO can also degrade the morale of a unit, reduce the target’s worth or value, or reduce the quality of adversary decisions and actions.</td>
</tr>
<tr>
<td>Destroy</td>
<td>To damage a system or entity so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.</td>
</tr>
<tr>
<td>Deceive</td>
<td>To cause a person to believe what is not true. [Military Deception (MILDEC)] seeks to mislead adversary decision makers by manipulating their perception of reality.</td>
</tr>
</tbody>
</table>
Why resilience? Isn’t risk management enough?

This section provides a review of the fundamental techniques of risk management. It also establishes that these techniques are insufficient for providing assurance that an organization is resilient to contested cyber environments.

There are four principal tools of risk management, including cyber risk management (Akintoye & MacLeod, 1997; Al-Bahar & Crandall, 1990). The four tools are avoidance, prevention and reduction (also called mitigation), retention, and transfer. But what do organizations perceive as risk (Cashell, Jackson, Jickling, & Webel, 2004)?

Organizations often perceive risk as a set of quantities that they can measure, cost shift, avoid, or otherwise measurably reduce (Flinn & Stoyles, 2005; Wallner, 2008). The downside(s) of those risks have some nominal negative impact on one or more aspects of the organization. The emphasis in traditional cyber risk management is reduction of the problem to one of two fairly simple models represented in equations (1)(MITRE, 2012a) or (2) (Stoneburner, Goguen, & Feringa, 2002).

\[
Risk = Probability \times Occurrence \times Impact
\]  
Equation 1 Risk as a function of the probability of occurrence and the forecasted impact

\[
Risk = f(Threat, Vulnerability, Asset)
\]  
Equation 2 Risk as a function of three variables: threat nature, vulnerability nature, and asset value

Importantly, none of these tools explicitly incorporates the notion of resilience: being able to recover from or adapt to the occurrence of a risk event. Resilience requires an explicit acknowledgement that risk cannot equal zero, and that risk varies over time. Mission assurance requires acceptance that nonzero risk means bad things will happen to an organization, despite the various avoidance, mitigation, retention and transfer measures in place. How organizations deal with that adversity is what assures their members and their...
leaders that cyber adversity is not an existential threat but a threat they can adjust to and function through. Without the explicit inclusion of both the ability to recover and the ability to adapt to the effects of the contested environment, traditional risk management is necessary for but not sufficient to establish mission assurance.

**Cyber threat literature**

What kinds of threats and problems exist that could create contested cyber environments? The introduction already alluded to at least two categories: man-made and natural. By natural, I’m referring to storms and other weather events, landslides, flooding, and virtually any other event for which humans are not the proximate cause. The other set of threats are man-made. Efforts to categorize these man-made threats, and their alter egos, vulnerabilities, have ranged from the taxonomies presented in the RISOS project (Abbott et al., 1976) to the four overlapping categories of the Protection Analysis project (Bisbey & Hollingsworth, 1978). Bishop built a taxonomy of six axes (1995) through using the categories of the Protection Analysis project as well as modified versions of Landwehr’s three categories (Landwehr, Bull, McDermott, & Choi, 1994). Howard’s dissertation (1997) has an extensive review of taxonomy attempts including the use of “results Categories” that mimic three of the five CNSS pillars of information assurance (i.e., confidentiality, integrity, and availability) by Cohen, Russell and Gangemi. Howard himself went on to develop what he called a process model whereby attackers use tools, to gain access to cyber systems, to create results to achieve some objectives (Howard, 1997). Hansman, like Howard, broadened his taxonomy to address specific vulnerabilities as well as three other dimensions of attack: vector, target, common vulnerability and exposure (CVE) entries, and payload or effect beyond the attack itself (Hansman & Hunt, 2005).

There are at least two degenerate cases of threat in the cyberthreat literature: (1) the nonexistent threat, in which case Equation 2 will become equal to zero (0); and (2) the computationally all-powerful adversary such as the Dolev & Yao adversary (1983) where the outputs of Equation 1 and Equation 2 are always greater than 0, and implicitly >> 0 while still \( \leq 1 \). More interesting are the arguments put forth that adversarial assumptions can lead to significant gaps in theoretical modeling (Gligor, 2008) and subsequent faulty policy decisions. Such arguments assert that adversary models should include the capabilities and
resources available as in (F. Cohen, 1999; Leblanc et al., 2011) as well as include adversary’s motivations (Gligor, 2008; Parker, Sachs, Shaw, & Stroz, 2004).

The efforts to classify and categorize cyber threats remain areas of continuing interest for a variety of audiences, researchers, and the military; Sun Tzu noted that knowing your enemy is essential to becoming a victorious general (2003). The intention in the preceding paragraphs was to illustrate a small portion of the efforts spent in that line of research—a complete rendering is well beyond this dissertation and not entirely beneficial to the point of focusing on the effects of contested cyber environments, independent of the agents and motivations of those agents.

**Rhetoric of catastrophic vulnerability**

There is hardly a week that goes by in the last several years when yet another news story discusses yet another cyber attack against some entity somewhere. Former US Defense Secretary Panetta is part of a long list of high USG official warning of dire threats to the US from “aggressor nation or extremist group” actors (Bumiller & Shanker, 2012). He is by no means alone, with the head of the National Security Agency and the new Cyber Command, General Alexander (Alexander, 2012; Roulo, 2012), the former Deputy Secretary of Defense Lynn (Lynn, 2010), and even the President of the United States all asserting that cyber security is a national security challenge with grave consequences if the country gets it wrong. Some US government representatives are less circumspect in their comments and conflate cyber attacks with an existential threat to the country (Thibodeau, 2010), feeding into a leader and media fed meme—dependence on IT equates to a loss of modern civilization if IT is degraded; a meme similar to the disaster myth of (Tierney et al., 2006).

These warnings may be rhetorical flourishes to overcome bureaucratic inertia, sincere efforts at forecasting the future, or simply appeals to historical analogy. In assessing the rhetoric, it is useful to ask, “What have been the outcomes of past events that had effects in the cyber domain? “There are various estimates of monies lost from cyber enabled financial crimes (Cashell et al., 2004; National White Collar Crime Center (NW3C), 2011), cyber enabled copying or destruction of intellectual property (Andrijcic & Horowitz, 2006; Nykodym, Taylor, & Vilela, 2005; G. S. Smith, 2004). There are national security estimates about years shaved off nation states’ research programs thanks to stolen plans from US
companies (Gorman, Cole, & Dreazen, 2009) and government agencies (Abreu, 2001; Kan, 2006). There are even reports of long-term attacks that copied unknowable amounts of data for which effects may never be known (Lennon, 2011; Perlroth, 2012; Thornburgh, 2005). What are the after effects of these and other reported events, aside from the prima fascia effects of monetary loss?

**Cyber effects and strategic war fighting**

There are public figures, pundits, authors, and former government officials, who declare that cyber war is already a reality. Richard Clarke’s book *CyberWar* is one example of such. But there is significant countervailing opinion—that not only is cyber war not here yet, but that the very word is a misleading and inappropriate conflation of distinct ideas. Security professionals such as Bruce Schneier and Marc Rotenburg concede that enormous quantities of cybercrime and espionage happen, but emphasize that though the threats are real, they are not war threats (Rotenburg et al., 2010). Despite the almost palpable fear in the testimony by GEN Alexander and Secretary Panetta’s public speeches, there are significant doubts that any enemy’s cyber capabilities can inflict significant long-term effects on the US—with equal doubts about US means to use cyber capabilities to war ending effect (Economist Editorial, 2012). It would not be the first time that pundits proclaimed that a technology represented a revolution in military affairs that makes warfare history irrelevant to the vision of future war—examples range from cross bows, to guns, to machine guns, to airplanes and long-range bombers, to nuclear bombs/missiles. The means change, decision and information flows expand and contract, but war continues, regardless of the perceived overwhelming technology edge of one side or another.

**Impacts of past large scale cyber–affecting events**

There is much gnashing of teeth in US defense circles about the speed with which China generated its modern stealthy fighters—especially after media reports of copied data moving from US defense contractors to China (Gorman et al., 2009; Reed, 2012; Staff Writer, 2012c). The Chinese creation of such a plane was not a matter of if, but of when. No technological advance, once exposed to the rest of the world, stays long in the sole possession of its creators. Creators execute the hard and expensive scientific efforts of proof of possible; copyists execute the efforts for reproduction and imitation. The concerns over Moonlight Maze (James Andrew Lewis, 2010), Titan Rain (James Andrew Lewis, 2005;
Thornburgh, 2005) and subsequent named intrusion sets into US government computer systems are also widely reported, frequently talked about, and yet rarely with specificity or even convincing generality. There are multitudes of mass media reports that USG cyber capabilities are infiltrated across the breadth of its unclassified systems—but if reports exist about the specific impacts of that infiltration, they are certainly not available to convince the general public of the harm done. Without the data points of harm done, it becomes difficult to assess the plausibility of the extrapolations of catastrophic impacts in the future. Indeed, the most recent report from the US Director of National Intelligence (DNI) reported the likelihood of a catastrophic attack is ‘remote’ and forecasting has now shifted to less grandiose outcomes (Clapper, 2015 #7696). Surely secrets have been lost, spies likely killed, citizens of countries imprisoned, but no credible argument has been made that those events would not have happened if all were quiet on the cyber front.

Degradation in cyber capabilities, and, sometimes, outright destruction of support infrastructure, are almost signature marks of modern large storms making landfall on our coasts. Hurricane Katrina and Super Storm Sandy both offer possibly instructive insights as to the cyber effects of natural environments. In Hurricane Katrina, of the many troubles faced by emergency management services, widespread loss of electricity as well as intermittent and total loss of communications are prominent in lessons learned reports (Guilford, 2010; Townsend, 2006). None of these reports point out loss of cyber and IT capabilities as a proximate cause of fatalities. None of these reports claim restoration of cyber capabilities would have significantly reduced the near term impacts of Katrina. The long-term health and demographic impacts New Orleans is still living with are several causal links away from cyber capabilities in the region—so the case for long-term effects of contested cyber environments has yet to be convincingly made to warrant the perceived levels of dread.

Super Storm Sandy’s impacts on emergency and other governmental services were equally profound in the short term. And despite the loss of electricity to over 7.9 million people (CBS/AP, 2012c) for days, and in some locations, even weeks (CBS/AP, 2012a), there are no lessons learned reports yet making the claim that a faster return of cyber and IT capabilities would have substantially reduced the widespread and long-term impacts of the storm. The loss of electricity, and other forms of damage, also impeded the reopening of mass transit systems (McCoy, 2012) that served millions of people a day (Goldman, Klopott,
& Vekshin, 2012). There has not been a credible declaration that their complete stoppage for
days, and only partial reopening, has destroyed New York, New Jersey and other served
areas—so exactly what would the long-term effects of a SCADA attack on mass transit
systems be? Water and sewage systems in shore communities from New Jersey (Reporter,
2012) to Connecticut (WFSB Staff, 2012) were negatively affected as well by the storm
through loss of electricity, flooding of facilities, uncontrolled spillage of untreated sewage
into waterways (Schwirtz, 2012). Again, no credible declarations of long-term catastrophic
damage to those communities from storm impacts to those utilities exist. This drives the
question of exactly how would a SCADA based attack on water and power systems degrade
our civilization?

Finally, there is a set of fears that large-scale cyber attacks could dramatically and
negatively impact the country’s and global financial markets. Prima fascia evidence is
usually from the Estonian attacks of 2007 (Ashmore, 2009; J. Davis, 2007), the Georgian
(Clark & Levin, 2009) and Lithuanian attacks of 2008 (Ashmore, 2009). On further review
however, the effects were greater in the public psyche and government outlook than in actual
damages to citizens or organizations within those countries. Enumerated damages included
delays of hours for monetary transactions and days for newspaper and government
information diffusion—hardly the cataclysmic outcomes of popular myth (Ashmore, 2009).

The closures of the NY-based markets from the 2003 power outages (Barron, 2003;
SEC, 2003), the 9/11 attacks (Masi, Smith, & Fischer, 2010), during and post Sandy (Kim,
2012) all had measurable impacts (e.g., USD 1.7 trillion in market losses (Navarro & Spencer,
2001)) and were more pervasive than any cyber attack thus far. However, the markets opened,
organizations that existed prior to those closures existed after the closures (with some
obvious exceptions of those housed exclusively in the twin towers), companies earned money,
paid taxes, and wrote off losses. In fact, there are precious few reports of public companies
driven to bankruptcy or other ruin due to cyber events—so exactly what are the long-term
effects of contested cyber environments?

In 2008 there were a series of undersea fiber optic cable breaks that decreased
regional bandwidth by 75% and in some instances logically isolated portions of the global
cyber communications networks (Masi et al., 2010). During that time, the US had major
combat operations on going in two theaters of war, and countries in the effected region were in the midst of conducting their routine international trading and running their national economies. Far from being unusual, undersea cable breaks are common, so much so that repair ships can spend 11 of 12 months a year at sea (Pole, 2009). With millions of end users, tens of thousands of organizations (governmental, public, and private), and dozens of countries effected (Masi et al., 2010), no country’s government has fallen, no stock markets suffered long-term crashes, no populations panicked into barbarity, and not a single war was started or ended due to loss of those capabilities. These breaks serve to create denial of availability and disruption of communications, but otherwise appear to generate little to no global effects and little to no long-term regional or local effects. The lack of empirical evidence of local or regional collapse, strongly suggests that extrapolations of catastrophic impacts are, at best, unsupported by evidence and at worst, appeals to fear of the unknown.

Appeals to analogical reasoning—cyber Pearl Harbor, Maginot Line, etc.

There is an obvious analogical fallacy in attempting to rally preparedness for contested cyber environments with a call to avoid a “Cyber Pearl Harbor.” The Japanese attack on Pearl Harbor had immediate and obvious effects such the death of over 2,400 sailors, soldiers, and marines, the sinking or damaging of 21 ships, and the destruction of over 180 aircraft (Staff Writer, 2012a). That strategic surprise (at least to the public) and tactical defeat, and the overlooked targets that could have had a greater long-term strategic effect (e.g., fuel storage and ship repair yards), set the strategic stage for the United States to enter the war, conduct full wartime mobilization and ultimately defeat the Axis powers. The country showed itself resilient to a localized kinetic attack as large as Pearl Harbor. The nation, with much hard work and sacrifice, ultimately achieved post-attack capabilities far beyond what it possessed pre-attack. A lesson of the “No More Pearl Harbor” analogies can be “Do not get caught unprepared and unaware.” What those analogies could also invoke are the memories of the other four (4) years of warfare that ended with enemies vanquished and America a dominant global super power. I am not asserting that a pervasive or prolonged contested cyber environment will lead to a victorious United States. I am suggesting that invoking “Pearl Harbor” to avoid surprise is a falling prey to the false analogy fallacy. Additional counter arguments to the analogy could include few people anticipated raids on Pearl Harbor, while watchers of daily news have heard stories of how easy it is for kids,
hacktivists, criminals and nation-states to exploit our vulnerable IT systems and cause us harm. Clearly if a large scale cyber attack comes, no national or company leaders should reasonably claim the idea of such an attack had never occurred to them.

Another analogical appeal is comparing computer network defense to France’s Maginot Line. The analogy frequently starts with the assertion that static computer network defense is as useless as the Maginot Line. The pre-World War II (WWII) Germans adapted to the presence of the Maginot Line with their decision to bypass the fortification zone—the ‘Line’ was a zone of defenses both laterally and in-depth, not simply a single line of defenses—in their May 1940 invasion of France. One of many military art and sciences lessons promulgated since 1940 is that static defense, with no ability to maneuver, surrenders the initiative to the offense—the attacking enemy. The attacking enemy can decide when and where to attack, while the defenders must defend their entire line at all times. A variant on this lesson is the perception that France placed all her war-delaying bets on the creation of a zone of defense impenetrable to expected attackers. With those bets, she deprived herself of defenses elsewhere. The lack of defenses along the French-Belgium border was what the Germans exploited—the Germans invaded France using a route through neutral Belgium.

These analogies, with their abstractions and omissions of details, are repeated within the computer security world in the egg-defense model (aka the M&M model)—a hard shell and soft unprotected interior. The hard shell usually refers to defensive infrastructure facing exterior threats such as firewalls, ingress & egress filtering and monitoring, and border intrusion protection and defense systems (IPS/IDS). The soft interior usually refers to the perceived lack of defenses throughout the rest of an organizations’ infrastructure and the portions perceived to have no direct contact with the outside world. These analogies are not wrong per se, but nor are they perfect fits in their choices of what to include and what to ignore or abstract. Indeed, examining each analogy shows points of comparison from which it is reasonably apropos to draw lessons learned. Examination also shows points of dissimilarity, some of which may be substantial enough to require yet another analogy, or other viewpoints.

Fundamentally, analogical reasoning is a useful tool in the human kit bag of reasoning skills. Ironically, if there is any cure to the problems of analogical reasoning—besides not using it at all—the cure lies in more analogical reasoning. Analogies, as
conceptual models, deliberately abstract away details of their subject matter. The application of multiple analogies, each with their flavors of ‘wrongness’ can provoke the recognition that there are few singular correct answers to extant problems—demonstrating George Box’s truism that “All models are wrong, but some are useful” (1979).

This section of the literature review is not intended to express an opinion that there are no effects in contested cyber environments. Nor that contested cyber environments will leave countries, companies, and people completely unaffected—the people of Estonia and Georgia were inconvenienced, scared, and forced to adapt. Cyber enabled espionage can, and likely has, led to death and imprisonment of spies, protestors, opposition parties, as well as the relations of those people. Companies have lost competitive advantages through loss of intellectual property, suffered loss of trust through data breaches, and some may have gone bankrupt—clearly effecting the shareholders, employees, customers, and whatever supply chains of which they were members. This portion of the review supports the notion that individuals, organizations, and governments need to spend more effort at making better estimates of ‘badness’ in contested cyber environments. It asserts that organizations, their leaders and workers, should not accept assertions that all contested cyber environments are inherently worse than other forms of risks to which they are accustomed, and to varying degrees, already resilient. Finally, it puts forth evidence that short of survivability challenges, contested cyber environments are not as fundamentally different in driving adaptation as some choose to believe.

**Related literature corpus and assessment**

**Overview**

The Literature Review’s Introduction highlighted multiple areas of related work. This section explains how I came to choose these sources from the corpus of texts, journals, and conferences I could have chosen.

When collecting sources and literature associated with resilience to contested cyber environments, it became evident that there is a multidisciplinary aspect to the approaches taken by researchers. I cast a fairly wide net of search terms using Google™, Google Scholar™, and Web of Science™, using back-citation tracing, and adjusting search terms and patterns while reviewing sources. I then input the data into the SNA software called
ORA™, from Carnegie Mellon University’s (CMU) Center for Computational Analysis of Social and Organizational Systems (CASOS). ORA™ (formerly called Organizational Risk Analyzer) supports application of social and network science methods and techniques to the collected data. The collected data included the following: authors, titles, publishers, journal/source, year, hyperlinks to original articles, and links to similar articles (as offered by Google Scholar™). Collection of citations, sources, and books via these web sources lead to over 14,839 unique sources for which this section provides a review and analysis. Details of the search methodology are in the Literature Review Bibliometrics section starting on page 238.

Semantic analysis

Prior to using latent dirichlet allocation (LDA) (Blei, Ng, & Jordan, 2003) and latent semantic analysis (LSA) (Laundauer, Foltz, & Laham, 1998) text analysis options in ORA™, my hypothesis was there would be links of varying strength between various aspects of resilience research. The hypothesized links, from intuitions based of 20 years as a computer scientist and over 10 years in the information assurance arena, are shown in Figure 9. I also expected that there would be three dominate forms of M&S discussed in the research literature, depicted as turquoise ovals in the figure.

I expected there would be links between the HRO, general risk management and the business continuity communities. I presumed there would be links between the business continuity and disaster management communities as well as the cyber risk management and the general risk management clusters of authors and topics. I also assessed there would be links between the business continuity community and the organizational behavior and learning communities—after all, continuity of operations in the face of adversity is a learning experience if ever there was one! Finally, I had a hypothesized that there would be stronger and more numerous links between the cyber risk management community and the M&S community, than between M&S and the other groups. Within the M&S field, I expected to find three main families of stochastic simulations: agent based, system dynamics, and discrete event. I also expected that the generalized cluster of M&S would contain many of the same references that serve as the foundational pillars of modeling and simulations.
The descriptive statistics for the collected citations and their respective meta-data are in Table 6.

This review is not a review of 14,800+ articles’ concepts. It is a demonstration through various network analytics that there are both links between various research communities and the absence of links that should reasonably exist through shared and common interests. Though LSA and LDA both require a researcher to assert, a priori, the number of clusters to which the algorithm should apply, I did not have strong evidence that Figure 9 was accurate—the intuitions are from 20 years exposure to the fields of computer science, computer engineering, risk management, information and computer security, operations planning and contingency planning. As such, I ran LSA using ORA™ for topic counts that ranged from 3 to 11, inclusive. I did the same for LDA using 5,000 iterations, a step size of 100, and \( \beta=0.01 \).
LSA (see also Figure 10 through Figure 15) was able to generate meaningful fully connected graphs with starting with 6 topics. The 6 topic LSA graph (Figure 10) depicts a fully connected graph though the intra topic links as well as the inter-top links are generally weak links. The 7 topic LSA graph (Figure 11) is also fully connected though the far left topic is only weakly connected to the remainder of the graph through a single shared node—“risk_assessment.” This graph however does reveal stronger intra topic links. The remaining topics have multiple inter topic links indicating shared concepts between topics. Of note is the topic of “simulation” does not occur using LSA until the number of topics rises to 10—indicating that Figure 9 is overly optimistic in establishing strong links between other key words. This lack of such a central topic for this dissertation is one indicator that the dissertation is providing an additional link between research topics.

<table>
<thead>
<tr>
<th>Total Number of articles</th>
<th>14,838</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of books(^2)</td>
<td>796</td>
</tr>
<tr>
<td>Number of ‘citations’(^3)</td>
<td>1,091</td>
</tr>
<tr>
<td>Authors</td>
<td>19,750</td>
</tr>
<tr>
<td>Concepts</td>
<td>4,276</td>
</tr>
<tr>
<td>Journals</td>
<td>5,013</td>
</tr>
<tr>
<td>Publishers</td>
<td>755</td>
</tr>
<tr>
<td>Schools</td>
<td>272</td>
</tr>
<tr>
<td>Websites</td>
<td>743</td>
</tr>
<tr>
<td>Years</td>
<td>43</td>
</tr>
<tr>
<td>Networks</td>
<td>53</td>
</tr>
<tr>
<td>Links</td>
<td>15,635,378</td>
</tr>
<tr>
<td>Total Density</td>
<td>0.75%</td>
</tr>
</tbody>
</table>

\(^2\) Generally identified within Google Scholar with the [B] or [BOOK] prefix in front of titles, as well as texts encountered by the author during readings and included in the search criteria as deliberate inclusion items

\(^3\) Generally identified within Google Scholar with the [C] or [CITATION] prefix in front of scholars, or citations pulled from web sites such as citeseer.org. These entries also do not generally have a readily accessible copy of the original source material available via the internet.
Since the 10 topic LSA groupings are the first to incorporate this key aspect of the dissertation (M&S), it is appropriate to conduct a comparison with the graphic shown in Figure 16 to the topic-connections shown in Figure 9. Within Figure 16, the light blue nodes are the topics (labeled with the concept with the highest value) and the yellow nodes are the highest valued concepts that the LSA algorithm found when performing single value decomposition (SVD) on the concept x document matrix. The links’ colors vary by value (red highest, blue lowest, with even distribution of color assignment) and the link value scales the link width.
This depiction of automated analysis compares somewhat favorably to the intuition depicted in Figure 9 for some clusters as well as some of the inter-cluster links. Supply-chains and the management of supply chain risk appear to align with the upper right topic of “model” while overlapping organizational learning. Modeling and Simulation does not appear as its own topic, but is a related node to the “response” topic in the center of the figure that also overlaps with organizational learning, but does not otherwise link any of the other topics—the cause of which remains unexplored. The originally expected notion of resilience appears in the “challenge” topic at the lower right. Related words of “case study” as well as the absence of any first or second order links to simulation are reflective of the room for improvement in the use of simulation in studying and assessing resilience. High Reliability Organizations, as sociotechnical systems appears to align with the LSA topic of “sys” (short for system) center-left of the figure. The associated terms disaster, emergency, and process lend credence to that alignment as well. The “Knowledge” topic, bottom center-right, aligns with the originally expected concept of generalized risk management while the “change” topic, bottom left, aligns with the cyber risk management. The originally expected organizational learning also appears to align itself with the LSA derived “practice” concept, though like the literature itself, the learning appears to be more market oriented than cyber event preparedness.
Figure 16 depicts graphically that there is indeed a gap between the research about organizational resilience (how organizations learn and adapt to adverse events) and research into cyber risk management. Until researchers begin to bridge these and other gaps, there is significant opportunity for duplicated work, missed findings, and other research inefficiencies. There is also room for better integrating general risk management research with resilience research and organization learning—the fit seems natural, and its conspicuous absence should serve as the basis for calls for broad agency announcements or requests for proposals.

LDA (see also Figure 17 through Figure 22) was unable to generate fully connected graphs until 13 topics. The 8 topic to 12 topic applications of the LDA algorithm generated graphs with 2, 3, or more components. Since the 13 topic LDA iteration was the first to generate a fully connected graph, a comparison with the intuition-based graphic shown in Figure 9 is appropriate. Like Figure 16, within Figure 22 the light blue nodes are the topics (labeled with the concept with the highest value) and the yellow nodes are the highest valued concepts that the LDA algorithm found when executing. The links’ colors vary by value (red highest, blue lowest, with even distribution of color assignment) and the link value scales the link width.

The upper left topic, labeled “cyber” is likely generated from the number of sources discussing the future of warfare augmented with cyber warfare. I had not included a “cyber war” node in the expected model, as it seemed a degenerate inclusion. The center-top topic of “worldwide” aligns, with overlaps, the expected organizational behavior node. The labeled “model” node in the upper right, a Quantitative is with overlaps, aligns with the general risk management. The “adaptation” node on the right-center of the figure aligns, especially when combined with its neighbor “info,” to the notion of organizational learning and adaptation. Of interest is the lack of direct link between these two nodes and the node in the center-bottom labeled “resilience.” This lack again indicates a gap between the resilience research and organizational adaptation and learning fields. There is a weak link between the “resilience” node and the system node on the left-center of the figure, also indicating a weak link between simulations and resilience areas of study.
Network Analysis

ORA™ uses network (graphs of nodes and links) analytics to help analysts identify Key Entities. Depending on the nature of the underlying quantity and nature of the underlying data, analysts can attain a higher confidence that their interpretations of the data attain at least face validity. With face validity, they can then use multiple forms of analysis to triangulate results and gain further confidence.

Key Entities

ORA™’s Key Entity functionality is unique across the various forms of social network analysis software and tools. The Key Entity functionality uses as many of the 170+ measures in ORA™’s repertoire, as the underlying data can support. For each measure, ORA™ stores a user-specified number of nodes (the default is 3) with the highest calculated values. For each set of measures applicable to the various node types (e.g., measures applicable to agents) in the data set, ORA™ then calculates the percentage frequency each of those high-value nodes appear in each measure. The ORA™ report then displays the number of nodes the user specified from the list of nodes’ with calculated values. The advantage to this approach is that individual measures may correlate with each other or have high inter-measure variability (Borgatti, Carley, & Krackhardt, 2006; Kathleen M. Carley, 2002d; Frantz & Carley, 2005). However, when nodes are consistently in the top-place ranks
aggregated across multiple measures, analysts can reasonably have more confidence in the relevance of those nodes to their questions of interest.

In set notation, Key Entities reports in ORATM follow the steps below. Equations (3) and (4) define the nodes and edges respectively. Equation (5) defines the set of possible measures applicable to the available nodes and edge.

\[
N = \{ \text{node} \} = \{ \, n_1, n_2, \ldots, n_{|\mathcal{N}|} \} 
\]

Equation 3 Node set definition in set notation

\[
\mathcal{E} = \{ \text{edges} \} \mid \mathcal{E}_{\text{edge}_{n_i}} \subseteq \mathcal{E} \land \mathcal{E}_{\text{edges}_{n_i}} = \{ \{ n_1, * \}, \{ *, n_i \} \} 
\]

Equation 4 Edge set definition in set notation

\[
\mathcal{M} = \{ \text{measure}(N, \mathcal{E}) \} \mid \text{measure}(N, \mathcal{E}) = \emptyset 
\]

Equation 5 Measures set definition in set notation

Each node-level measure (as distinguished from a network-level measure that generates a single value) generates a set of real values where each value’s place in the set corresponds to the place in the node set of the node being assessed as shown in (6). In other words, a real value \( b_1 \) in (6) corresponds to a value calculated using node \( n_1 \) in (3).

\[
\forall m \in \mathcal{M}, m = \{ R \} = \{ b_1, b_2, \ldots, b_{|\mathcal{M}|} \} \mid b_i = m(n_i, \text{edges}_{n_i}) 
\]

Equation 6 A measure’s output definition in set notation

For the measure \( m \) calculated in (6), the top \( x \) calculated values are retained, realizing that each of those values represent the node from which it was calculated. This retention of the top \( x \) values is shown in (7) for any arbitrary measure \( m \) as is the mapping from real value \( b_1 \) to node \( n_1 \). The set of nodes corresponding to the top \( x \) calculated values is shown in (8).

\[
\mathcal{X} = \max_{1..x} (m) = \{ \forall x, \max_x (b_1, b_2, \ldots, b_{|\mathcal{M}|}) \} \mid b_i \rightarrow n_i 
\]

Equation 7 A set of maximum values from a measure’s output in set notation

\[
\mathcal{Y} = \{ n_x, n_y, \ldots, n_z \} 
\]

Equation 8 A set of node identifiers corresponding to maximum values from a single measure in set notation
Across all relevant measures, the algorithm builds a set of top rank nodes as shown in (9). The algorithm then builds a set of values using every node in the graph. It counts the number of times each node in $\mathbb{N}$ appears in the set $\mathcal{Z}$, divides by the number of measures and achieves the percentage of measures the node has achieved a top ranked value. This set of values is shown in (10). Finally the algorithm takes the top $x$ values from $\mathcal{T}$, relates them back to their contributing node identifier, and presents the identifiers to the analyst as shown in (12).

$$\mathcal{Z} = \{\mathcal{Y}_m, \forall m \in \mathcal{M}\}$$  \hspace{1cm} (9)

Equation 9 A set of measures’ results as sets of node identifiers in set notation

$$\mathcal{T} = \forall n \in \mathcal{N}, \frac{\sum_{m} \left\{ \begin{array}{ll} 1 & n \in \mathcal{Y}_m \\ 0 & \text{otherwise} \end{array} \right\}}{\mathcal{M}}$$  \hspace{1cm} (10)

Equation 10 Calculating the frequency of occurrence a node is in the maximum value set of all relevant measures

$$\mathcal{KE}_{freq} = \max_{1..x} (\mathcal{Y}) = \left\{ \forall x, \max_{x} (T_1, T_2, ..., T_x) \right\} | \mathcal{T} \rightarrow n_i$$  \hspace{1cm} (11)

Equation 11 A set of maximum frequency of occurrence values in set notation

$$\mathcal{KE} = \{ke_1, ke_2, ..., ke_x\}$$  \hspace{1cm} (12)

Equation 12 A set of node identifiers corresponding to maximum frequency of occurrence values in set notation

When performing this function across the data collected for the corpus of citations, ORA™ helps identify the following key entities. The figures below offer another way to visualize the key entities describe by the equations above. In particular and of note, there are no dominant (i.e., an author or Journal or other entity that reaches higher than fifty percent (50%) across all the various applicable measures. This result reinforces the perception that there is significant room for research, Journals, and publishers to increase their cross-discipline research as well as apply and absorb completed research from outside their primary areas of focus.
Figure 24 Key Entity 'Author'

Recurring Top Ranked Author - Dissertation Related Literature

Figure 25 Key Entity 'Journal'

Recurring Top Ranked Journal - Dissertation Related Literature
Co-Authorship Networks

The full visualization of the Co-Authorship Network (i.e., the graph such that an edge between two author nodes indicates a shared authorship and the weight of the edge indicating the number of distinct co-authorship efforts) is a undifferentiated ball of nodes and edges with the vast majority of nodes involved in dyads or triads with edge weights of one (1). However, when I added a progressively higher filter on the edge weights that hide all edges below the filter threshold, the graph rapidly degenerates into very small clusters of authors who write with each other. At filter weight of less than 2 (see Figure 29) there are a small
number of such clusters that form author-strings or more traditional core-periphery networks. With the filter set to hide edges with less than a weight of 3.5 and hiding isolates, a disconnected graph remains (see Figure 29 for the unzoomed view, and Figure 30 for the zoomed in view) making it easier to see that very few cross-domain co-authorship efforts exist in the realm of organizational reliance to adverse cyber environments. When I added pendant nodes back into the graphs, the co-authorship networks remain unconnected (as expected) except for clusters of prolific authors, as shown in Figure 31. Adding the pendants into the graph depicts the increased opportunity for collaboration by adding related authors.
Co-Citation Networks

The full visualization of the Co-Citation network (i.e., the graph such that an edge between two article nodes indicates a shared citation and the weight of the edge indicating the number of distinct shared citations) is more akin to a head of cauliflower (see Figure 32) than an undifferentiated ball of nodes and edges. There are clearly distinct clusters of well-cited articles surrounded by increasingly less sparse connections between shared article citations. The co-citation network for books and articles (see Figure 33) shows a much less connected collection of co-citations between articles and books with the vast majority of nodes involved in dyads or triads with link weights of one (1).

Figure 32 Co-citation network of Article x Article, no filtering
This Overview has presented bibliometric and textual analysis views of the related literature supplemented with visual renderings and graphs of the information. While useful, particularly to depict areas of overlap and underlap, these views need additional supporting evidence via explication and discussion of specific trends, texts and authors. The remainder of this section provides a review of literature from each of the clusters identified above.

**Risk management**

As noted in the beginning of the section *Why resilience? Isn’t risk management enough?*, traditional risk management starts with the idea of risk avoidance (K. D. Miller, 1992). There are other traditional tools of risk management besides avoidance with common ones being: prevention and reduction, retention, and transfer (Akintoye & MacLeod, 1997; Al-Bahar & Crandall, 1990).

An organization can avoid a risk if that is a feasible course of action; if there is a risk a rocket will blow up during launch, the organization could choose not to launch the rocket, much less attempt to build a rocket. If the organization’s mission is to launch rockets, clearly this is an infeasible choice. Organizations who missions are supported by cyberspace capabilities may decide it is equally infeasible to abandon the use of those capabilities in pursuit of their own requirements.
If an organization can reduce the *probability of occurrence* or the *impact* term in Equation 1 (on page 23) to near zero, the organization could drive the overall risk to near zero. To continue the rocket launching analogy, the organization may reduce the probability of an explosion during through rigorous testing of systems and subsystems throughout their performance envelopes prior to an actual launch. For cyberspace-enabled organizations, they can reduce probabilities of certain types of event occurrences (e.g., catastrophic engine malfunction, hard disk failures and loss of data) despite being unable to reduce all events’ probabilities to zero. Similarly, if the *impact* term drops to near zero, there is a greatly reduced requirement to reduce the *probability of occurrence* to near zero—as the impacts are negligible. For the rocket-launching organization, they may be able to reduce the impact of a launch vehicle explosion by having some sort of payload evacuation mechanism such that only the launch vehicle suffers the impacts—akin to the crew escape system on the Saturn V. For a cyberspace enabled organization, having fail-over systems and fail-over processes in place may make the impact on primary systems negligible.

Prevention and reduction are close cousins to avoidance. How much prevention and reduction an organization should pursue with respect to reducing risk from contested cyber environments is a question with as many answers are there are variations in organizational situations. Significant effort has gone into creating and publishing cyber risk management frameworks. Contributors to the field have been standards bodies (NIST, 2012), Federal Funded Research and Development Corporation (FFRDC) such as MITRE (MITRE, 2012c) and Software Engineering Institute (SEI) (Alberts & Dorofee, 2010) as well as individual researchers (Hoo, 2000; Pfleeger, Predd, Hunker, & Bulford, 2010; Ralston, Graham, & Hieb, 2007). Many of these frameworks offer extensions of the basic models of Equation 1 and Equation 2.

Some risk management frameworks involve a cycle of identification of possible threats and the vulnerabilities of organizations’ assets to those threats, identification and implementation of mitigation measures, and a calculation of residual risks (Hoo, 2000; NIST, 2012; Wallner, 2008). Each of these has a component of the cycle that requires an organization to reduce one or more terms in the respective equations through implementation of one or more controls—measures put in place by the organization to cause a reduction in equations’ terms. These risk-mitigation phases of the various frameworks’ cycles help reduce the original level(s) of risk to level(s) that decision makers are willing to accept. Researchers and security practitioners often
refer to this acceptance of risk after efforts of reducing it as the acceptance of residual risk. Of course, this comfort level is subject to the usual limits of human decision heuristics: 1) representativeness, 2) availability of instances or scenarios, and 3) adjustment from anchor (Tversky & Kahneman, 1974). It also is important to recall that the extensions are cycles, and are not supposed to be a one-off execution of the process but a periodic, if not continuous exercise (Siegel, Sagalow, & Serritella, 2002).

Retention may often be a more practical form of risk management than the other three tools, as well as the fundamental last active step of a risk management process. An example of risk retention is the fact that the US Government retains the risk of loss of physical assets such as buildings, equipment, and other tangible items ("48 CFR Parts 202, 203, 211, et al.," 2011; USHR, 2012). The USG does not purchase insurance as a protection mechanism. There are undoubtedly many reasons for this governmental lack of transfer, but difficulties with enumerating the number of physical assets that embody the cyber and IT infrastructure (such as those experienced with the Navy/Marine Corps Intranet (NMCI) (Musich, 2001)), the states of repair, and precautions against loss or damage surely contribute to the challenge. I found no evidence of efforts to study whether the US government could sufficiently inform an insurance company of the types and quantities of cyber assets the government owns and operates; presumably the probability it could do so is small.

Risk transfer is a time-honored form of risk management by which the risk becomes a commoditized item: there are sellers and buyers of risk, with each side of the transaction attempting to reduce losses. The various insurance industries that exist around the globe are in the business of selling protection from downside risk, while charging their customers enough to cover losses and make profits. Cyber risk transfer markets are beginning to develop with supporting research (Bandyopadhyay, Mookerjee, & Rao, 2009; Böhme, 2005; Böhme & Kataria, 2006) at the consumer level and at the corporate level (D. R. Cohen & Anderson, 2000)—though a Chubb Group of Insurance Companies survey found 65 percent of companies forgo cyber risk transfer (Chubb Group of Insurance Companies, 2012).

Of these four tools, risk transfer and the acceptance of residual risk come closest to explicitly acknowledging that risk is not zero, and that there is nonzero probability of negative events occurring. Being able to rehearse for and adapt to those negative events is not explicitly
part of the tools for cyber risk management, as such rehearsals and adaptations frequently occur outside the areas of expertise of the cyber SMEs.

**Risk management frameworks**

Risk management frameworks develop a common language for practitioners of risk management. Many frameworks have names or identifiers published by standards organizations such as ISO 31000 *A Structured Approach to Enterprise Risk Management (ERM)*, NIST Special Publication 800-30 (Stoneburner et al., 2002) or SEI’s Enterprise Risk Management Integrated Framework (Alberts & Dorofee, 2010). Some of these are deliberately general and do not explicitly reference cyber risk management, while others are very specific about including IT and cyber in risk management planning, such as the DoD Directive 8500.01E *Information Assurance (Department of Defense, 2007)* and CJCSI 6510.01F *Information Assurance and Support to Computer Network Defense* (Joint Staff J6, 2011).

Miller (1992) also developed a comprehensive risk management framework specifically for international companies which are using information technology to enable their operations. Despite this use of IT, the primary references to technology in Miller’s framework seem to relate to whether competitors will produce a technical innovation in products or processes, not how the organization adapts to degradation of its IT capabilities.

The frameworks above, and others I am aware of, implicitly treat change in the operating environment as a nearly ever-present phenomenon. The implicitness is communicated in the admonishments to risk-managers and organization leaders to treat risk management as a never-ending cycle of activities. However, the lack of explicit planning and rehearsing for low-probability negative events reduces the efficacy of these frameworks in establishing mission assurance. Another drawback to frameworks, despite the as-designed cyclic nature, is the data supporting assessment with compliance to the framework tends to be snap-shot in time data, not a continuous data stream or constant assessment. This lack of continuous assessment means that compliance to framework requirements are lagging indicators of risk reduction where the lag could be days to weeks and sometimes longer. This lag between data collection and transformation to information also reduces the confidence in mission assurance assessments.
High Reliability Organizations (HROs)

What makes HROs fundamentally different from learn-through-experience/experimentation organizations — those able and willing to learn from errors with less than existential consequence (La Porte & Consolini, 1991)? Early research of HROs used examples of high-costs-of-failure operations such as US Navy aircraft carrier flight deck operations and Federal Aviation Authority (FAA) control tower operations as motivating examples (La Porte & Consolini, 1991; Roberts, 1989). Two characterizations from (Roberts, Rousseau, & La Porte, 1993) encapsulate those difference: (1) HROs tend to focus on process reliability because outcomes are impossible to achieve without the process—carrier flight deck operations would be an exemplar; (2) HROs tend to have expectations of high-tempo for sustained periods of time while maintaining their ability to do so—air traffic control being a prime exemplar. Research into HROs over the last thirty years has flourished, extending into fields as diverse as medical practice (Ash, Berg, & Coiera, 2004; Baker, Day, & Salas, 2006), and disaster and emergency planning (Crichton et al., 2009; Lally, 2013) as well as post facto explorations as to event causation (e.g., Shrivastava’s book on Bhopal (1987) as well as post space shuttle Challenger research (Kathleen M. Carley, 1991)).

One of the more interesting, though difficult to model, aspects of HROs is the multiple forms of self-organization they take on. Structures that correspond to routine operations differ from those in peak-loading conditions, which in turn differ from in extremis conditions (Roberts, 1989, 1990). Unfortunately, for organizations that do not perceive themselves as operating in these conditions, there appears to be less willingness to transform successful HRO practices than might be fruitful. Though the specific organizations in this dissertation are not HROs, the ability of agents in the simulation of this dissertation to not be restricted to a single form of organizational structure can represent this simultaneous structuration seen with HROs.

Supply Chain Management and Resilience

Supply Chain Management (SCM) is a field that enjoys a rich history despite dating to the early 1980s (Cooper, Lambert, & Pagh, 1997). A founding idea behind SCM was the interorganizational control of costs associated with inventory (Cooper et al., 1997; Min & Zhou, 2002). The International Center for Competitive Excellence defined SCM as “the integration of business processes from end user through original suppliers that provides products, services and
information that add value for customers” (Cooper et al., 1997). Implicit in this definition, and its surrounding literature, is the need to control, mitigate, and adapt to the risks faced by companies with supply chains. Though Cooper et al.’s literature review reveals differing opinions of scope, she points out that there is widespread agreement about the need for information systems integration, planning and control activities. Indeed, of the seven authors she presents comparing/contrasting SCM and business process reengineering perspectives (Houlihan, Stevens, Cooper and Ellram, Hammer & Champy, Andrews and Stalic, Hewitt, and Towers), all consider IT structure supporting information flow a critical component of their research and business practices (Cooper et al., 1997). Yet the notion of resilience, of ensuring these optimized and efficient systems can adapt to unexpected environments is present only by implication, suggesting a gap in awareness of the need to balance optimality and efficiency (Gunderson, 2003; D. D. Woods & Branlat, 2011).

One of the principal tools of exploration in this field is empirical study. One popular alternative to empirical study is computerized M&S (Swaminathan, Smith, & Sadeh, 1998). Min and Zhou’s review of M&S of SCM divides the various forms of M&S into four categories; the traditional deterministic and stochastic models, a hybrid model of the two, and IT-driven (2002). The use of IT-driven models (e.g., near-real time monitoring of various stages in the chain, as well as near-real-time adjustments to process) also exposes SCM practitioners to risks, in particular the triad of confidentiality, integrity, and availability (CIA) (G. E. Smith et al., 2007). For supply chains that use IT to drive or enable specialization versus generalization, any event that creates effects within the CIA triad puts those chains at risk of imbalance (D. D. Woods & Branlat, 2011).

Reductions in costs, improvements in customer service, faster speed to market, and more efficient use of resources are all measurable by-products of the exploitation of robust cyber environments (G. E. Smith et al., 2007). Given these documented benefits, how do SCM practitioners protect themselves for the inevitable problems within cyber environments?

As early as 2003, calls emerged to shift from the traditional views of risk assessment, business continuity planning, and crisis management to an approach where ‘risk management’ is embedded with SCM and other operations—to enable earlier anticipation and mitigation to risks (Jüttner, Peck, & Christopher, 2003). Jüttner also advocated for looking at the points of origin for
risk, which fell into three categories: organization, network, and environment. The links between organizations in the supply chain, the network source, and environmental risks (e.g., natural events, socio-political events) drew particular attention as neglected areas of research (DHS, 2011; Jüttner et al., 2003; G. E. Smith et al., 2007). DHS and several of the national laboratories are making progress with constructing simulations that address portions of the supply chains, in particular the electricity and gas markets, by considering them as complex adaptive systems (CAS) (Peerenboom & Fisher, 2007). Though these and other CAS simulations have worked at integrating market reactions into these efforts, there remains a key challenge of integrating nonindustry specific actors as well as human agents into the simulations.

There remains the ongoing challenge of assessing the impacts of contested cyber environments generally (DHS, 2011), and within supply chains specifically. Published consequences from the supply chain community of practitioners are primarily anecdotal in nature (G. E. Smith et al., 2007), or estimations of costs that leave much of their methodology to the imagination of the readers. In short, SCM practitioners are still working on identifying how to assure themselves of the efficacy of their business practices and models in contested cyber environments.

In response to these difficulties and the growing awareness of dependencies on entire networks of related organizations and technologies, supply chain management literature has seen a growth in the idea of disruption management (Pereira, 2009) as championed by Christensen (Christensen, 2006).

**Computer Security and Resilience**

In many surface-level discussions of computer security, the participants implicitly assume that secure cyber systems are resilient, as no attacks can affect them. A single question will generally disabuse the conversationalists of their simplistic, and naïve notion, “Security from what, for whom, for how long, and at what opportunity costs?” Such a question often results in muttering and stumbling attempts to elucidate an answer. Alternatively, security requirements could drive the discussion (Bishop, 2003) of what constitutes ‘security’. We’ll defer whether to measure, what to measure and how to measure efforts to meet these requirements to later in this dissertation.
Inherent in any security plan should be some residual acknowledgement of possible failure—of one of the dreaded D’s (i.e., destruction, denial, degradation, disruption, and deception). Short of destruction, an organization should be confident in the ability to continue functioning despite the event, ideally during but minimally after the event is over. This is the “recover from” “misfortune or change” portion of the definition of resilience at the beginning of this paper. But is the ability to restore functionality what a computer scientist, system developer or programmer perceives when she hears ‘computer security?’ Depending on her background and the context, she could perceive a definition akin to a “reasonable assurance that the complete system will function (only) as required and intended, despite hostile activity” (Horning, 2009). This definition, especially in computer science circles, supports component level design and analysis (Bishop et al., 2011). It’s a reasonable starting place for a profession inculcated with problem decomposition and step-wise refinement. But the definition shortchanges unplanned interactions between technology components as well as unplanned use by humans (Rinaldi, Peerenboom, & Kelly, 2001). Nor does Horning’s definition support a holistic approach to security as a sociotechnical problem, where humans and human organizations interact with components of technology and webs of interconnected technology. This web of interconnected humans and technology is extremely close to characteristics of HROs—minus the tendency of HROs to focus on process before product.

Earlier, I used a definition from Merriam-Webster for resilience. The definition implicitly requires that the event or events affecting the system not totally destroy it—pieces and parts maybe, but if the overall system of interest no longer exists, is clearly not resilient, nor was it survivable. Unlike (Bishop et al., 2011; Pimm, 1984), it is important to note that the “or adapts to” portion of definition offers the possibility that the system or systems of interest do not return to pre-event performance! In cases where a system is capable of adapting, it is feasible, and possibility desirable, that the adaptation is permanent, or at least not abandoned at the first opportunity. In addition to Merriam-Webster, a quick review of other definitions, and more importantly ways of assessing those definitions, is appropriate.

Assessing resilience

Assessing resilience is essential for communicating to organizational leaders how its definition applies to their organization. A quick review of ways various industries and research
realms define the concept is fruitful at this point. In ecology circles, generally applied to eco-
systems and the study of species, there appear to be two main variants to the definition of
resilience (Perrings, 1998). One is a measure of how fast a stable system returns to its
equilibrium following a perturbation, and there is no definition of resilience for unstable systems
(Pimm, 1984). This makes the concept easily susceptible to measurement, in some unit of time,
and requires some idea of whether the measured time is acceptable or not. The other variant
assesses the magnitude of perturbation that a system can absorb while still persisting, what
Holling referred to as “ecological resilience” (1973). This form of assessment may be
measurable, depending on the nature of the perturbation. M&S readily supports Pimm’s
definition while Holling’s definition is more applicable to an assessment of cybersystem
survivability more than resilience—a lack of persistence implies system destruction, and a
destroyed system is clearly not able to recover from or adapt to the perturbation.

Within the computer technology industry and academia, resilience also has multiple
interpretations. In the virtualization of computer resources industry, resilience is another flavor
of availability (Gilpin, 2008). In this incarnation, the ‘up-time’ of the capability or systems of
interest is also easily measured, both during and after cyber attacks or events. This is clearly not
a sufficient indicator of adaptability to misfortune or change, as there are plenty of events that
could disrupt organizations without making the systems they use nonavailable. Others theorists
assert, “Being resilient to an attack, [means] we are stressing the ability of the system to recover
from the impacts of this attack or at least to maintain the potential of autonomous recovery”
(Bishop et al., 2011). The first half of this definition is akin to Pimm’s return to equilibrium,
though Bishop’s has a clear expectation that the equilibrium is equal to the pre-event levels. Such
an expectation may be too restrictive, as complex adaptive systems should be able to learn new
behaviors, and once learned, they cannot reasonably be un-learned. Nor is it clear that a universal
requirement for autonomous recovery is necessary for all organizations.

Some in business management community, view resilience as a capacity for continuous
reconstruction and requires systematic preference of innovation over perpetuation of the status
quo (Hamel & Välikangas, 2003). This can also be reflected in Equation 13. This definition
might be measurable and assessed assuming reasonable estimations of each term are feasible,
while organizations desire to decrease the magnitude of the denominator while increasing the
magnitude of the numerator. In other words, reducing the time, expense, and emotional energy associated with transformations is a clear way of increasing resilience in uncertain environments.

$$Resilience = \frac{f(|\text{strategic transformation}| \times \text{strategic transformation}_{\text{frequency}})}{f(\text{time, expense, energy}_{\text{emotional}})}$$  \hspace{1cm} (13)

Equation 13 Resilience as a function of the magnitude of transformation, the frequency of transformation, time, expense, and emotional energy

The American National Standards Institute (ANSI) defines resilience as “the adaptive capacity of an organization in a complex and changing environment” with two explanatory notes, one for organizations and one for systems. Note 1 states: “resilience is the ability of an organization to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.” Note 2 states “resilience is the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must” (American National Standards Institute (ANSI), 2009). All three of these slightly different flavors do not immediately lend themselves to straightforward measurement or assessment. Organizations have to have a coherent model of their functions and structure to support this definition or find and use measurable proxies for these concepts.

The US government is also not immune to creating definitions, as the Department of Homeland Security (DHS) defines resilience as “for cyber defense purposes, having sufficient capacity to simultaneously collect or receive and assess security information, execute any ACOA (Automated Courses of Action] make alterations to the ACOA as needed, and sustain agreed upon service levels” (DHS, 2011). This definition, like the ANSI definition, presupposes a way of measuring organizational capacities as well as predicting the impacts of various events on those capacities. While definitions must of necessity be concise, the DHS definition simply begs for clarification and expansion—which requires another 29 pages to explicate.

What is clear from discussion so far is that resilience to contested cyber environments means a number of things to different audiences—there is no singular definition applicable across all possible contexts. What is apparent however, is interested audiences should not treat resilience as an isolated static measure independent of time. Instead, it incorporates time, effects of perturbations, and the maintenance of function during perturbations and adaptation to those
perturbations. There are no Newtonian laws of adaption that require the adaptations be permanent. Nor are there universal asymptotic equations constraining adaptations to pre-perturbation levels of performance. These realizations lead us to a short review of non-HRO treatments of organizations learning and behavior—how collections of people learn and behave, especially in stressful environments.

**Organizational Learning and Behavior**

Industry and academia have well established that organizations learn and Huber’s literature review does an excellent job reviewing the history of experiential learning of organizations (Huber, 1991). There is significant evidence that the learning is nonlinear, is often based on myths and stories, and is at times mal-adaptive (Cyert & March, 1963; B. Levitt & March, 1988; March, 1991). There is also evidence that organizations behave differently in ambiguous and unambiguous environments (March & Olsen, 1975; Padgett, 1980) as well as evidence that individuals call on different relationships and information gathering mechanisms in times of uncertainty and ambiguity (Saint-Charles & Mongeau, 2009). The entire field of organizational learning and behavior is well beyond the scope of this review, so the remainder of this section is constrained to research on organizational learning and behavior that includes organizations’ information technology and cyber resources.

Researchers have shown organizational structure (both formal and informal structure) effects learning and adaptation. Padgett found that the heads of hierarchies can best influence their organizations by focusing more on who they pick to run their various subordinate organizations than on trying to make decisions themselves (Padgett, 1980). Organizational structure, the relationships and links between the members of the organization and links between organizations, also plays a role in learning. Hierarchies, though non-optimal in many measures of organizational performance, tend to be more resilient to certain types of turbulence (e.g., personnel turnover/turbulence) than other structures (Kathleen M. Carley, 1992). The reader may also recall the seeming paradoxes associated with HRO research contrasted with traditional organization theory. The first is HROs tend to use significant quantities of advanced technology that requiring specialization yet HROs also exhibit high degrees of interdependence that requires generalist understanding. The second is that HROs tend to have high task interdependency despite operating in high variability environments (Roberts, 1989, 1990).
Wade & Hulland, in their review of organizational learning and information technology literature (2004), used the resource-based view (RBV) of organizations. In this view, IT systems are tangible assets while the knowledge to run those systems, the knowledge stored in those systems about how the organization runs and operates are capabilities of the organization. He also discusses multiple research products that demonstrate that IT systems, and the capabilities represented in them often play distinct roles in gaining initial competitive advantage and sustaining long term advantage (Wade & Hulland, 2004). Unfortunately, Wade, Huber, nor Damanpour’s (1991) literature reviews include research on IT dependent or enabled organizations when those resources are degraded or no longer available. Neither does the meta-analysis model built by Damanpour’s (Damanpour, 1991) integrated inclusion then disruption of cyber resources.

Research on the use of information technology, or other cyber capabilities, to enable communications within organizations, especially to facilitate adaptation also has a robust history. Empirical studies on adoption of information technology go back over thirty years (Orlikowski & Gash, 1994). The data sample driving this review has over 130 articles with more than 100 citations each in the data sample dealing with technology relating to adaptation and learning. Miller showed that even in primitive environments, any communications mechanism will improve performance and having more robust communications will increase performance (J. H. Miller & Moser, 2004), while Carley (1995) and Haythornthwaite (2005) have studied and demonstrated that mass communication technologies can encourage common homogeneous culture, but only as an eventuality—that the near term can suffer in increase in heterogeneity and loss of consensus. Martin et al asserted via simulation that the degree of information error and the degree of communications network intermittency interact to reduce decision accuracy in organizations across random structural designs (Martin, Morgan, Joseph, & Carley, 2010). Interestingly, they discern statistically significant impacts on decision accuracy by communications media only in the extreme cases of information error (e.g., all accurate, all inaccurate) (Martin et al., 2010), which implies that organizations are resilient along this measure of performance. This finding of accurate learning and performance being independent of organizational structure is in contrast to Carley’s determination that training and structure are statistically important, as is the location of the communication’s breakdown (Kathleen M. Carley, 1991).
Surprisingly, there appears to be very small quantities of research directed at use of IT in degraded or destroyed environments. Among the studies of adaptation to disruption and loss of communications networks are those focused on flow disruption (Saltysiak & Levis, 2012) and development of decision support systems (Saltysiak & Levis, 2012; Snediker, Murray, & Matisziw, 2008) and efforts to setup taxonomies of mission impacts from cyber events (Grimaila, Mills, & Fortson, 2013; Musman, Temin, Tanner, Fox, & Pridemore, 2010).

A close cousin to organizational learning is organizational assessment. There is a field of science that has grown up around assessing organizations, what they have learned and their effectiveness at their missions. Unfortunately, organizational effectiveness, in addition to going through a near death experience in the early 1980s, has the problem of exactly who is measuring what and to what standards (Cameron, 1986). In addition, like resilience, there is the debate about when to study—before events or after. In the case of organizational effectiveness, researchers tend to examine well-established companies with less emphasis on new and dynamically expanding organizations (Quinn & Cameron, 1983). In the case of examining resilience to contested cyber environments, researchers focus on the direct monies loss, estimates of future monies missed, and estimates of indirect costs such as damage to reputation or trust. These have the disadvantage of being poor and opaque proxies for organizational impacts (DHS, 2011; Jüttner et al., 2003). Judging by scarcity of published materials, researchers are not yet looking at the ways the companies adapted to the contested environment and demonstrated resilience to their misfortune(s).

As noted by Huber (1991), the organizational learning literature has an enormous breadth, and over 20 years later there are still gaps to explore. The documents in the collected sample, plus additional and refined searching, have still lead to a paucity of research of organizational learning and adaptation to contested cyber environments. This paucity seems to be a natural area of research to bridge between resilience engineering, risk management, and cyber risk management.

**Social Network Analysis (SNA), Metanetworks, and Dynamic Network Analysis (DNA)**

The representation of collections of humans interacting with other humans, and the systematic study of those representations is an old and widely practiced field. Since the mid-twentieth century, a common description of this study has earned the name Social Network
Analysis (Freeman, 1977, 1979). These representations most frequently take the form of single mode networks, or graphs comprised of links and nodes. In single mode networks, each node is a person and the people under study belong to a single class—there are not distinct types of people (Wasserman & Faust, 1994). Two mode networks within traditional SNA usually refers to the interactions of two distinct types or groups of people (Wasserman & Iacobucci, 1991), such as doctors interacting with nurses, or intravenous drug users interacting with their sexual partners (Williams & Johnson, 1993). A sample of SNA metrics that researchers apply to the graph models of human interactions is below in Table 8 drawn from (Kathleen M. Carley, 2011).

Multimode analysis usually supports a richer understanding of the human groups of interest than single mode and I provide a brief review below.

Metanetworks and Metanetwork Analysis are an extension of SNA and a modification of the definition of multimode network. In metanetworks, multimode networks are networks with numerous distinct node types, e.g., agents, resources, tasks, and knowledge. From the three-node type instantiation (Krackhardt & Carley, 1998) it progressed to a four-node version (Kathleen M. Carley, 2002a; Kathleen M. Carley & Krackhardt, 1999) similar to that shown below in Figure 34 to the nine (9) node-type version shown in Table 7 (Lanham, Morgan, & Carley, 2011a) derived from (Kathleen M. Carley, 2002a; Diesner & Carley, 2005) which is its current state.
Table 7: Nine (9) node metanetwork and their internode link interpretations

<table>
<thead>
<tr>
<th>Networks</th>
<th>Agent</th>
<th>Knowledge</th>
<th>Resource</th>
<th>Task</th>
<th>Event</th>
<th>Organization</th>
<th>Location</th>
<th>Role</th>
<th>Belief</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>Information “What informs what”</td>
<td>Training “What resources are needed for training”</td>
<td>Knowledge Requirements “What knowledge is task critical”</td>
<td>Education “What event teaches what”</td>
<td>Organizational Knowledge “What org knows what”</td>
<td>Knowledge Location “Where is what learned”</td>
<td>Role Requirements “What must be known to perform what”</td>
<td>Resource Requirements “What beliefs are required to use what”</td>
<td>Resource Beliefs “What beliefs are required to use what”</td>
</tr>
<tr>
<td>Event</td>
<td>Event Precedence “What events happen before what”</td>
<td>Organizational Responsibility “What org is putting on what”</td>
<td>Event Location “Where is what event”</td>
<td>Role-Event Location “What roles are often present at what”</td>
<td>Organization Location “Where is the organization”</td>
<td>Organization Role “What org has what roles”</td>
<td>Belief Requirements “What beliefs require what tasks”</td>
<td>Belief Attendance “What beliefs influence participation at what”</td>
<td>Belief Influence “What beliefs influence what”</td>
</tr>
<tr>
<td>Organization</td>
<td>Inter-Organization “What org works with what”</td>
<td>Organizational Location “Where is the organization”</td>
<td>Organization Role “What org has what roles”</td>
<td>Significant Locations “Where is associated with what beliefs”</td>
<td>Significant Roles “What roles are associated with what beliefs”</td>
<td>Belief Influence “What beliefs influence what”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Proximity “What is near what”</td>
<td>Location Roles “What roles are common where”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles</td>
<td>Inter-Roles “Who knows what”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Beliefs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4 (Lanham, Morgan, et al., 2011a) and derived from (Kathleen M. Carley, 2002a; Diesner & Carley, 2005)
In Figure 34, a four node type metanetwork is shown. Each oval represents one of four node types, with DMU being equivalent to “decision making unit.” Implicitly in this diagram, there exists links amongst DMU nodes, intra-task links, intra-resource links and intra-knowledge links. Those intra-task links represent, usually, task dependencies or task precedence networks. Intra-resource and intra-knowledge links can also represent resource and knowledge dependencies or even compositions or aggregations of resources and knowledge. The various labeled relationships are depicted unidirectional, but there is no definitional requirement that a modeler must maintain such a convention. The development and refinement of metanetwork model construction and analytical development has been a hallmark of Carley’s research group at CMU’s CASOS (Kathleen M. Carley, 2003).

![Four-node metanetwork](image)

**Table 8: Common SNA metrics and their interpretations**

<table>
<thead>
<tr>
<th>Measure Name</th>
<th>Definition</th>
<th>Meaning</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Degree Centrality</strong></td>
<td>Node with most connections</td>
<td>In the know</td>
<td>Reducing information flow, ID sources of intelligence</td>
</tr>
<tr>
<td><strong>Betweenness</strong></td>
<td>Nodes in most best paths using symmetric data</td>
<td>Connects groups</td>
<td>Typically has political influence, though may be too constrained to act</td>
</tr>
<tr>
<td><strong>Eigenvector centrality</strong> (Bonacich, 1972a, 1972c)</td>
<td>Nodes connected to other well connected nodes</td>
<td>Strong social capital</td>
<td>ID nodes that can mobilize other nodes</td>
</tr>
<tr>
<td><strong>Closeness</strong></td>
<td>Nodes closest to other nodes</td>
<td>Rapid access to all information</td>
<td>ID nodes to best acquire/transmit information</td>
</tr>
<tr>
<td><strong>Betweenness Centrality</strong> (Freeman, 1979; Freeman, Roeder, &amp; Mullholland, 1979)</td>
<td>High betweenness, low centrality</td>
<td>Connects otherwise disconnected groups</td>
<td>Go-between; Reduction in activity by disconnecting groups</td>
</tr>
<tr>
<td><strong>Authority Centrality</strong>  (Kleinberg, 1999)</td>
<td>Sum of hub scores from in-link / hub score</td>
<td>Subject Matter Expert</td>
<td>ID nodes that others recognize as SME on one or more subjects</td>
</tr>
</tbody>
</table>
Metanetwork notation in Carley et al.'s research, as well as this dissertation is below.

$$\mathbb{A} = \{Agent_1, \cdots, Agent_m | m \geq 1\}$$, the nonempty set of all agents in the metanetwork

$$\mathbb{K} = \{Knowledge_1, \cdots, Knowledge_j | j \geq 1\}$$, the nonempty set of all knowledge in the metanetwork

$$\mathbb{R} = \{Resource_1, \cdots, Resource_k | k \geq 1\}$$, the nonempty set of all resources in the metanetwork

$$\mathbb{T} = \{Task_1, \cdots, Task_k | k \geq 1\}$$, the nonempty set of all tasks in the metanetwork.

$$\mathbb{A}\mathbb{A}(i, j) = \begin{cases} 1 & \text{ if } i \neq j \\
0 & \text{ otherwise} \end{cases}$$, matrix of relationships between agents

$$\mathbb{A}\mathbb{T}(i, j) = \begin{cases} 1 & \text{ if } i \neq j \\
0 & \text{ otherwise} \end{cases}$$, matrix of agents with their assigned tasks

$$\mathbb{A}\mathbb{R}(i, j) = \begin{cases} 1 & \text{ if } i \neq j \\
0 & \text{ otherwise} \end{cases}$$, matrix of agents with access to resources

$$\mathbb{A}\mathbb{K}(i, j) = \begin{cases} 1 & \text{ if } i \neq j \\
0 & \text{ otherwise} \end{cases}$$, the matrix of knowledge possessed by agents

$$\mathbb{T}\mathbb{K}(i, j) = \begin{cases} 1 & \text{ if } i \neq j \\
0 & \text{ otherwise} \end{cases}$$, the matrix of tasks linked to their supporting knowledge

Carley et al have also been vigorously applying the metanetwork perspective to over time models (Kathleen M. Carley, 2003; Kathleen M. Carley & Lee, 1998; Lin & Carley, 1997; Schreiber & Carley, 2005) at the same time that longitudinal network analysis remains a vigorous field of research for both understanding network evolution (Graham, 2005; Skvoretz & Fararo, 1995; Ter Wal & Boschma, 2007; Tushman & Romanelli, 1985; Zeggelink, Stokman, & Van de Bunt, 1996) as well as network change detection (McCulloh, 2009; I. McCulloh & K. M. Carley, 2008; I. McCulloh, Daimler, Eric, & K. M. Carley, 2008). When adding the time dimension to metanetworks, the definition of dynamic network analysis becomes clear: the study of multimode and multiplex networks over time. The expansion of quantifiable measures into the metanetwork framework supports the calculation of generalized measures across the multimode network such as performance as accuracy, shared situation awareness (Graham, 2005; Graham, Schneider, Bauer, & Bessiere, 2004), knowledge and communication congruence and workload and cognitive demand (Kathleen M. Carley & Pfeffer, 2012a, 2012c). Dynamic metanetworks,
like their SNA antecedents, also support bi-directional links though the various SNA software products treat this data differently and the researcher must decide if the calculation of the metric against the available data is meaningful (Wei, Pfeffer, Reminga, & Carley, 2011).

**Modeling and Simulation**

As discussed in the “Supply Chain Management and Resilience” section, Incorporating uncertainty into supply chain models and attempts to understand HROs are fairly robust fields of research (Pereira, 2009). Where SCM modeling still needs to grow is the explicit inclusion of contested cyber environments as a cause of uncertainty. Within DHS sponsored research, simulation of disruption of critical infrastructures with SymSuite (Brown, Riolo, Robinson, North, & Rand, 2005), SMART++ (North, 2000), and RINSE (Leblanc et al., 2011) is well advanced for exploring inter-dependencies of complex physical infrastructures. Incorporating socio-political components into any of the tools does not appear to be a part of their follow-on work.

Modeling complex adaptive systems (CAS) is also a healthy area of research applied to a great many fields, from finance markets (Markose, 2005) (see (Hommes, 2001) for a markets as CAS literature review) to critical infrastructure (Rinaldi et al., 2001). These efforts have ranged from exploring organizational designs to cope with communication breakdowns (Kathleen M. Carley, 1991; DHS, 2011) to sociotechnical models such as OrgAhead (Effken, Brewer, Patil, Verran, & Carley, 2005; Lee & Carley, 2004; Louie, Carley, Haghshenass, Kunz, & Levitt, 2003), SimVision (Emery, 2002; ePM, 2012; R. E. Levitt & Kunz), and Construct (Kathleen M. Carley, Joseph, Lanham, Morgan, & Kovalchuck, 2014; B. Hirshman, St. Charles, & Carley, 2011; B. R. Hirshman, Kovalchuck, & Carley, 2008)

OMNeT++ (OMNeT++ Community, 2012) and NetSim (ns-2) are examples of technology-focused, discrete event simulation environments that enables M&S of networks at the technical system and component level: networked devices, communications channels and messages on those networks (2012). There are numerous other examples of technology-focused simulations, from OPNET Modeler from Cisco, to University of Illinois at Urbana-Champaign’s Real-Time Immersive Network Simulation Environment (RINSE) (Leblanc et al., 2011), to the seventeen network emulators listed in (Lochin, Pérennou, & Dairaine, 2012), that all provide evidence of the field maturing greatly since Cohen’s lamentations about the sad state of cyber
security M&S (F. Cohen, 1999). With these capabilities, researchers are able to construct models of technical components of infrastructure, as well as organizations’ sets of other cyber resources and assets (e.g., servers, terminals, other IP-enabled devices). With those models they can choose various forms of network degradation (e.g., congestion from a denial of service attack, loss of packets from a noisy transmission medium or other adversarial effect), analyze the effects on the effected systems, the network as a whole, as well as identify 2nd and 3rd order effects in their models.

Process-level modeling of business processes has also been, and remains, an active field of research. Colored petri-nets (Levis, Carley, & Karsai, 2011) and colored petri-nets over time (Pflanz, 2012; Pflanz & Levis, 2012) as well as time-influence nets (Levis et al., 2011) have incorporated various levels of cyber attacks into their efforts to gauge impacts on organizational capacities and decision time lines. Machine-level processes, independent of human-controlled actions, have also been explored in the development of rate control services (Gligor, 2005) and load-balancing redirection (Pai et al., 1998; Wang, Pai, & Peterson, 2002). Human-enabled process modification (e.g., employing off-line backup capacity) is also apparent in (Pflanz, 2012; Pflanz & Levis, 2012) as a way of assessing the sustainability of time-sensitive missions in cyber degraded environments. What these process-based models omit though are the individual agent level adaptations to the environment—disaggregating agents is not a feature of the above modeled processes and flows.

Each of these tools, to greater and lesser degrees, can help construct scenarios where researchers or analysts can model an organization’s technology assets and assess its technical resilience to the chosen perturbations. But what of the nontechnology assets? Every organization has people, processes, resources, data, information and tasks that, to some degree or another, must go on even during “misfortune or change.” RINSE has been used by the USG during a Livewire exercise (Leblanc et al., 2011), the DoD’s Bulwark Defender attempts to train staffs and commanders in process adjustment and efforts to inject communications effects servers into exercises continue (Wihl, Varshney, & Kong, 2010)—though the risk of participants’ misperceiving an attack as a simulation malfunction is ever present. There is an apocryphal story in DoD simulations community Incorporating that very real risk.

*Exercise participants in a virtual and constructive simulation, on perceiving a malfunction in the simulation, headed to lunch. On their return from lunch, they*
discovered the enemy had destroyed their simulated units and equipment. On demanding an explanation from the simulation support staff, the players learned they had misdiagnosed the cause of several events, failed to report or explore the possible causes of the events, and subsequently had their units die as a result of leaving their workstations.

Multimodel modeling is another technique to assess organizational resilience in contested cyber environments. Researchers use multiple models to address multiple portions of the problem space: technical details, information diffusion, social influence, forecasting effects, and forecasting the efficacy of remediation’s and adaptations. These models exchange information about their own inputs and outputs to help enrich the overall modeling effort (Kathleen M. Carley, Geoffrey P. Morgan, Michael J. Lanham, & Jürgen Pfeffer, 2012; Kathleen M. Carley, Geoffrey P. Morgan, Michael J. Lanham, & Jürgen Pfeffer, 2012; Elder & Levis, 2010). These works have shown a way to having models work in tandem, though they are not inter-operable per se. The models share information, and most importantly can serve as means of validating the outputs of each other—when systems with very different internal processing generate congruent results, analysts can have higher confidence in the feasibility of the results. Examples of the tools used in the above modeling efforts include: OMNet++, Construct (an agent based belief and information diffusion simulation) (Frantz & Carley, 2007; B. Hirshman et al., 2011), CAESAR III (a C2 design tool) (Levis & Perdu, 1996), and Pythia (a timed influence net simulation) (Wagenhals & H., 2001; Wagenhals, Levis, & McCrabb, 2003; Wagenhals & Wentz, 2003). With the combination of these tools, researchers were able to assess multiple aspects of resilience: the ability to continue functioning during a perturbation, assess the magnitude of various effects within the modeled organizations, and forecast the adaptations needed by the organization to perform as best it could in its simulated environment.

Yet another example of multimodeling was the co-use of ORA™ and MONOPATH. In this merger of tools that analyze social networks and telecommunications networks, researchers found that including message passing paths from social-networks in a resilience analysis, organizations can improve the message delivery by a factor of five without gross changes in end-to-end latency(Bigrigg, Carley, Manousakis, & McAuley, 2009).

An example of a process centric M&S approach to assessing resilience is Pflanz’s work with colored petri nets (Pflanz, 2012; Pflanz & Levis, 2012). With this approach, a modeler builds information flow paths and then executes them to assess the model against various
measures of performance and effectiveness. With timing information included in the information path, this technique has shown that time-sensitive missions (e.g., a military unit’s ‘time-sensitive targeting’ using GPS-enabled munitions) are not supportable when key portions of the model are ‘denied’ (e.g., GPS jamming). He also showed that organizations that are IT enabled may have no reduction in capacity with one attack on their systems, though they have zero residual capacity to absorb any additional misfortunes.

M&S of contested cyber environments tends to fall into three camps. The first is the discrete event simulation that operates at bit/byte-level and/or the telecommunications-network-level. These simulations help computer scientists and engineers identify specific failures of components, protocols, or individual systems and IT engineers and organizations identify actual or potential portions of the network that exhibit nondesired behavior. They can help simulate the technical failures associated with a contested cyber environment, but do not incorporate any of the cognitive learning and adaptation functions of the organization. The second camp is the organization model that supports examination of the organization(s) at varying degrees of aggregation from the individual person up to teams and groups—but those rarely incorporate explicit and implicit dependencies on IT and information residing on that IT. Even more rarely do those organizational simulations support the experimental analysis of how the individuals, teams, and organizations as a whole adapt to the degradation or destruction of the IT assets they perceive they are dependent on. The third camp is a process-centric set of modeling capabilities. In this camp, detailed, time-dependent models are built per process-of-interest. When the models are complete, what-if scenarios offer insights to possible effects of future scenarios.

Each of the above camps adds value to the M&S communities to which they belong. Unfortunately the absence of an ability to model the cognitive adaptations of organizations to the use and loss of their cyber capabilities remains a capability gap in the research of organizational resilience!

**Gaps in research into organizational resilience in contested cyber environments**

From the beginning of this literature review, I have developed a case to justify the importance of studying organizational resilience in contested cyber environments. There should be few reasons for arguments against the notion that modern, 21st century organizations, especially in the industrialized first world, are increasingly using their information technology
and cyber capabilities in ways they had neither predicted, nor are they fully appreciating the multitudes of 2nd and 3rd order consequences of such use.

Despite this growing use of IT, I also developed a case that doomsday, apocalyptic, and other predictions of existential threats are intemperate, and place the advocates for those views in a less credible position than they could otherwise maintain. Instead, I set the stage for a reasoned and deliberate inter-disciplinary study of organizational resilience in contested cyber environments—both man-made and naturally occurring.

This allowed us to transition into an explanation of how I collected sample articles and texts associated with what I had initially assessed would be primary candidates for inter-disciplinary studies: supply chain management, business continuity, general risk management, cyber risk management, organizational learning, organizational behavior, and modeling and simulation. Through semantic network analysis and network analytics, I demonstrated that 13,000 collected articles show weak connections between cyber risk management and risk management, weak connections between general/global risk management and organizational learning, and an even weaker link between organizational resilience and organizational innovation.

Next I offered a literature review of cyber risk management, organizational resilience, organizational learning, as well as modeling and simulation applied to each of those three areas. The literature reviews, while necessarily brief, illustrated that despite the breadth of research in each area there are far fewer areas of commonality and shared references than intuition originally suggested. There are gaps between the fields of research of organizational learning supported by IT and the loss of that IT once the organization has grown accustomed to it. There are gaps in the M&S support to both technical dependency modeling and cognitive modeling of humans using the technology. Finally there are gaps between the risk management communities (cyber and general) and organizational learning—as evidenced by the continued successes bad actors enjoy exploiting human vulnerabilities in organizations.

Reliance on a set of capabilities represents a risk to organizations that have few or no alternatives. Mitigating risk is a natural outgrowth to being aware of it, and preparing for the eventuality of the undesired events should also be a natural part of organizational operations. With practice, an organization gains confidence in its abilities—it builds an experiential store of
knowledge from which it can draw actual lessons as well as extrapolate to unfamiliar situations. Practice is, of course, expensive, opening the door to the use of M&S as an expense mitigation compared to live experimentation with organizational elements and assets otherwise occupied with daily missions. With confidence and ability, organizations can assure themselves, their leaders, and the organizations they interact with that they are resilient to misfortune, that they can adapt and overcome adversity.
Data and Models

Introduction

This chapter will introduce the methodology for collecting data for use in this dissertation. It will also introduce the process and contributions for rapidly turning that data into multimode (multiple node types) and multiplex (multiple types of links between nodes) organization models for assessing mission assurance in contested cyber environments. The chapter will also present processes and rationales for the modifications to the collected data to transform the empirical models into inputs for the agent based simulation, Construct (Kathleen M. Carley et al., 2014). In the literature review and research for this dissertation, I have not found evidence of using this methodology and its generalization for organizational modeling in cyber contexts. Nor have I uncovered evidence of its application to DoD doctrinal source material and the use of its outputs in mission assurance contexts. This rapid modeling approach represents one of the principal contributions the dissertation to the field of mission assurance and organizational resilience to contested cyber environments.

Prior to providing the detailed discussion of the data collection and processing, it is useful to see a high level view of what will happen to that data in the workflow of the dissertation. Figure 35 provides such a view, with the left most rectangle representing this chapter, and the blue ovals representing supporting or specific activities. The Data-to-Model (D2M) process (Kathleen M. Carley, Bigrigg, et al., 2011; Lanham, Morgan, & Carley, 2014; Lanham, Morgan, Carley, & Levis, 2011) is a defined sequence of steps for researchers to use, with the support of automation, to rapidly ingest unstructured and semi-structured data and convert that data into SNA and metanetwork-based models for analysis using graphic theoretic techniques. The process is in the oval labeled D2M in Figure 35. Its counter-part, the oval labeled Stylized, represents the necessity to compare organizational models with some form of baseline from which we can perform meaningful comparisons and assessments of differences. These baseline organizations come from standard SNA methods of creating random graphs that model abstract organizations. The stylized models use the empirically identified quantities of node types, node set sizes, and edge densities. The next chapter, Network Analytics and Resilience, provides the detailed discussion of metrics against the static models generated within the D2M-process and the static stylized models—the Calculate Metrics rectangle in Figure 35.
The in-depth discussion of Performance as Accuracy (PaA) and Shared Situational Awareness (SSA) is also in the next chapter.

**Organization—a working definition**

For the purposes of this dissertation an organization is a collection of decision-making units (DMU) (aka specific agents) and roles (aka general agents). The organization also includes the DMUs’ supporting IT systems and capabilities as well as other resources. The organizational definition also includes the tasks and knowledge of the organization’s members as well as their beliefs, specified events and enumerated actions. Each of the above named categories of entities is, in their respective models, a node type. Any arbitrary node is a specific instance of a node type. The model, to be accessible to graph theoretic techniques, also includes the relationships between these various nodes and their node types. There may also be multiple relationships in that two different edges representing two distinct types of relationships may link nodes together. Subsequent paragraphs will explain how I gathered data to construct the multimode and multiplex models of organizations under test.

There are two types of organizations in the dissertation, both derived from the D2M process: strategic and tactical. The two are shown in Figure 35 as the two leftmost ovals, with the rest of the workflow standardized and applied to both models. I present the data sources for the D2M derived models next.
Organizations’ Self-Documentation

Organizations frequently describe themselves in various ways, not all of which are aligned with the perceptions of their members or nonorganizational observers. A common mechanism for an organization to describe itself is in terms of its mission statement: for whom does it work, what it does, why it does what it does, when does it do its work (or to whose schedule), where does it do its work, and how does it accomplish its work. Mission statements, if they exist, are excellent starting points for new arrivals to the organization as well as observers to gain a level of understanding about the organization.

Another mechanism organizations use to describe themselves are documents they write for their various intended audiences. A vision statement from the chief executive officer (CEO), or other principal leader, targets not only outsiders with whom the company interacts or wants to interact, it can serve as a common point of reference for internal audiences. A combination of mission statements and vision statements frequently serves as the beginning of organizational culture—a shared set of knowledge (Kathleen M. Carley, 1994). They can also serve as the starting point for organizational modeling as well as help scope the models in this dissertation.

An additional way organizations describe themselves is via organization charts. These often represent subsets of people and suborganizations as blocks connected via lines. The lines and the relative position of the blocks often indicate direct and indirect reporting chains (e.g., chains of command), information flows, and functional specialties. These charts assist organizations’ formal depictions of themselves and relationships between included elements or people. What the charts rarely depict is the myriad of individual persons in each subelement—the autonomous humans that ideally subscribe to and help implement the organizations culture and mission.
The Data to Model (D2M) Process—an Overview

Using Figure 36 as a breadcrumb, the D2M-process, is the first step in the creation of organizational models to use to answer the questions of interest in this dissertation.

From the mid-1970s onward, there has been a growing effort at developing a theory of semantic networks—that networks of disambiguated words (as nodes) related to each other (using links) can represent human knowledge (W. Woods, 1975). To a large degree, this effort was in support of the then-expanding field of artificial intelligence (AI) and bridging the gaps in approaches between linguists and AI researchers (Hartley & Barnden, 1997). By the early 1990s, semantic analysis had matured to the point that meanings were measurable on multiple dimensions (e.g. connectivity, conductivity, and consensus (Kathleen M. Carley & Kaufer, 1993)) as well as supporting research into multiple mechanisms to visually represent (Gloor & Zhao, 2006; Hartley & Barnden, 1997) such networks.

By using text documents generated by various organizations and authors as sources for semantic networks, it is feasible for a researcher to gain insight not only into the possible overlaps in content but also perceptions of overlap in responsibility (Ekstrom & Lau, 2008) for organizational tasks. Semantic networks can also help represent the authors’ mental models as they wrote the various documents (Diesner & Carley, 2005, 2011) as well as help automate the acquisition of relational information for members of an organization (Gloor & Zhao, 2006; Mergel, Diesner, & Carley, 2010).

As previously mentioned, the D2M-process (Kathleen M. Carley, Bigrigg, et al., 2011; Kathleen M. Carley, Columbus, Bigrigg, Diesner, & Kunkel, 2011; Diesner & Carley, 2004;
Lanham et al., 2014) is a rapid machine-assisted transformation of a collection of text documents (labeled DoD Doctrine and Pubs in Figure 37) into a metanetwork model (Panzarasa, Carley, & Krackhardt, 2001). It includes an ontological classification scheme of nine (9) categories into which each concept will fit. Through this process, the researcher constructs an indirect model of the collected documents. These models are reflections of the concepts and ideas the authors’ of the input documents were attempting to communicate to their respective audiences.

The D2M-process, as applied to this problem domain and source material domain, required adaptation of the methods the sources cited above describe. Shown in Figure 37, the process began with a thesaurus that CASOS staff, faculty, and students developed using both hand encoding as well as machine learning techniques (i.e., conditional random field ontological categorization). Through a D2M Wizard within AutoMap, this figure represents the completely automated first-round process of text cleaning, removal of stop words, and other processing steps performed for the user. From this wizard, AutoMap generates multiple products a researcher uses to determine if the model of the text is sufficient to their needs. The products include semantic networks, often referred to as collocation networks of words within a sliding window of specified size, suggested ngram lists, suggested review lists, and suggested acronym lists. A key product is the first generation metanetworks (per text if of interest, as well as the union of all texts’ models).

It is frequently the case that the first generation metanetwork is insufficiently developed to explore or resolve questions of interest, and that was certainly true in this dissertation. For these cases, the human-aided D2M-process begins with thesaurus refinement as shown in Figure 38 and linked to Figure 37 via the “A” off-page connector in the flowchart. To develop a second (2nd) through nth iteration of a metanetwork that can help resolve the research question of interest, I used the defined process labeled “1” in the Figure 38 flowchart. This requires extracting the concepts from the Wizard generated lists into a dissertation thesaurus. For each of the three organization models, discussed in the next section, I developed an additional thesaurus to adjust the overall scope of the model and its contents. While developing these thesauri, it was necessary

---

5 AutoMap processing time per file for some steps is approximately logarithmic in file length. Because of this growth in processing times, Figure 37 depicts a subprocess whereby I combined the retrieval of the files as pdfs, the extraction of text from those pdfs using pdftotext, and the splitting of the extracted text files into chunks no bigger than 64KB.
to develop two (2) capabilities not yet in AutoMap: the application of regular expressions as well as case sensitive application of thesauri.

Figure 37 Data to Model (D2M) Wizard applied to any input corpus

DoD self-documentation has numerous references to other documents that frequently follow patterns of use. Through development and application of Perl Regular Expressions to convert these document identifiers into ngrams, it was my expectation that I would be able to identify which of the sources appeared to have the most impact on the overall model development. DoD document authors also frequently use acronyms, which commonly overload standard English words (e.g., IT, WHO, OPS, POP), which they stylistically render in all capital letters. To cope with these two characteristics of the input corpus, I modified the standard CASOS D2M-process by adding the defined process labeled “2” in the Figure 38 flowchart. The details of these steps are in the Pre-processing DoD corpus section of Appendix 3. Of particular note at the end of this overview are some of the specific tangible deliverables of the dissertation. The specific deliverables, as shown in Figure 38, are the pre-processing scripts for regular
expressions and case sensitive application of a thesaurus, the dissertation thesaurus, acronym/case sensitive thesaurus, and the model-specific thesaurus. All of these deliverables are free of restrictive intellectual property rights as a work product of the USG, though I do ask that future users of the deliverables acknowledge the products’ origin! I have also made these thesauri and the scripts available on my personal web page at http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support.

Figure 38 D2M refinement applied to DoD input corpus

Two D2M generated DoD organizational models

The DoD is an organization that expends enormous effort in documenting itself. One of the ways it does this is through the writing and distribution of doctrine documents. DoD includes Joint doctrine in most professional military education courses that have mixed-Service audiences
and senior service members. The military departments (e.g., Army, Navy, Air Force) also teach Service-specific doctrine in Service-provided professional military education courses, where emphasis is placed on the Service rather than Joint operations. The hierarchy of primacy for doctrine within the DoD is Joint followed by Service (i.e., Army, Navy, Air Force, Marine), in accordance with the intent of the Goldwater-Nichols DoD Reorganization Act of 1986 (Baldwin, Picavet, & Reiners, 2009). The Goldwater-Nichols Act emphasized the need and imposed requirements for Services to train and fight as joint entities, and not fiefdoms of expertise and noncooperation.

There are three principle levels of military organizations: strategic, operational, and tactical (which is not in the dissertation). These three levels are identical to what the US military education system often calls the three levels of war. Using two of these levels of war demonstrates the generalizability of the approach from mid-sized organizations to globally dispersed organizations. Figure 39 is a simplified and scoped depiction of the strategic and operational levels of command, supported by the descriptions in following sections. I’ve color coded the diagram with Joint organizations in purple, USAF organizations in blue, civilian components of strategic decision making in read, white, and blue. Mixed colors represent organizations with mixed origins. I also provide a comparison of the descriptive statistics for the D2M Wizard generated models and the iterative refinement generated models. For those interested in replication of the effort, the lists of documents used to build each of these three models are Appendix 1 as well as the bash shell scripts used to collect the documents and transform them into text on my personal web site at

http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support.
National Command Authority (NCA) to Combatant Commands (COCOM)—the strategic level

The strategic-level organizations I modeled are the National Command Authority (NCA), US Strategic Command (USSTRATCOM), US Cyber Command (USCC), and US Central Command (USCENTCOM). These are shown in Figure 40. These first three are driven by the definition of strategic warfare.

The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. [Joint Staff J7, 2010 #7253]

The NCA (i.e., “the President and Secretary of Defense together with their duly deputized alternates or successors” (NCA, 2013) supported by the National Security Council (NSC), the Joint Chiefs of Staff (JCS), and their respective staffs) is at the top of this level of war. Equally clearly, Strategic Command, to which NCA, through JCS, has assigned long-range military assets (e.g., B2 bombers) and space assets and from which those assets take authoritative orders is part of this level’s model. US Cyber Command (USCC and USCYBERCOM), a sub unified joint command (U.S. Cyber Command Public Affairs, 2010) of US Strategic Command, has the responsibility to assure US freedom of action within cyberspace. I then chose USCENTCOM from the pool of six (6) geographical combatant commands (GCC) the US operates. This choice derives primarily from the fact that USCENTCOM continues to be engaged in a shooting war.
with large numbers of US forces, as well as small elements of allied and coalition forces. This engagement often drives resource allocation within USCENTCOM that might have been different had they not had forces in contact with enemy combatants. The colors coding in the graphic remain the same: purple for the ‘Joint’ units; a blend between Service colors (i.e., blue for USAF) for ‘Joint’ units predominately from a particular service; and solid colors for units from a particular Service. There are no doctrinal colors for NCA and NSC, so I simply render them in red, white, and blue.

![Figure 40 Simplified figure of USG strategic level organizations](image)

**COCOM to Numbered Air Force level (NAF)—the operational level**

The operational level of war is the large, and often amorphous, span of military operations and commands between the obviously strategic and the obviously tactical. The official definition is below.

*The level of war at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas (Joint Staff J7, 2010h).*

In practice, this is the portion of the chain of command that spans from the regional combatant commands (COCOM) to the first echelon of the tactical level, the division or Service-specific equivalent (e.g., a USAF group, a USN battle group, or a USMC division). For this dissertation, I modeled USCENTCOM and its Numbered Air Force (9th US Air Force). Instead
of modeling the 9th AF’s assigned Groups or Wings, I leveraged previous work (Lanham, Morgan, & Carley, 2011b, 2011d) and modeled its Air Operations Center (609th Air Operations Center), operating as a Combined Air Operations Center (CAOC). These organizations are shown in Figure 41.

![Diagram](image)

Figure 41 Simplified figure of COCOM and USAF operational level organizations

With the creation of US Cyber Command, the relationships at this level of command have become increasingly complicated. Complications are from at least two sources. The first is the cyber related direct reporting from tactical elements directly to USCC. The second is the perception, from multiple quarters, that USCC can and should issue cyber related orders directly to tactical elements operating under USCENTCOM’s command jurisdiction without de-conflicting their noncyber operational impacts.

Preceding work (Lanham, Morgan, et al., 2011b, 2011d) to this dissertation successfully modeled one portion of a USAF operational level organization called the Air Operations Center (AOC) and depicted above as CAOC. Figure 42 is an extract from the Air Force Instruction (AFI) 13-1 (USAF, 2005) that depicts the doctrinal organization of the AOC. Figure 43 depicts the hierarchy of the organization as well as the cross functional area teams as extracted from the AFI during the D2M process.
There were a total of 139 doctrinal files for the construction of the strategic and operational models. A tabular summary of the input corpus I used for these models is shown in Table 9 with descriptives of the sizes of each corpus (in megabytes) depicted in Table 10 and Table 11. It is worth noting that there are several open research questions about this selection, as well as any particular sample of any particular corpus when constructing these types of indirect
models. Open questions include: What distribution(s) exist for each of the nine (9) ontologies normalized by MB or KB? Are those distributions domain dependent? Does the sample of documents generate distributions that align with the domain of interest? What are the impacts on processing time (normalized by processor count and available RAM) of the sizes of the input documents? These questions, while interesting, and brief discussions of each are in the Limitations and Future Work section of the dissertation—they may assist in demonstrating to particular audiences additional facets of model validity as well as offer expectation management with the use of the word ‘rapid’ in the dissertation title.

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>58</td>
</tr>
<tr>
<td>Operational</td>
<td>81</td>
</tr>
<tr>
<td>Total</td>
<td>139</td>
</tr>
</tbody>
</table>

Table 9: Number of input files per model

Table 10: File Sizes (MB) descriptives per model/level of war – part 1

<table>
<thead>
<tr>
<th></th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Std. Error</th>
<th>95% Confidence Interval for Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>58</td>
<td>1.7682</td>
<td>1.36599</td>
<td>.17936</td>
<td>1.4090</td>
</tr>
<tr>
<td>Operational</td>
<td>81</td>
<td>1.6211</td>
<td>1.27510</td>
<td>.14168</td>
<td>1.3392</td>
</tr>
<tr>
<td>Total</td>
<td>139</td>
<td>2.4079</td>
<td>2.50609</td>
<td>.17677</td>
<td>2.0594</td>
</tr>
</tbody>
</table>

Table 11: File Sizes (MB) descriptives per model/level of war – part 2

<table>
<thead>
<tr>
<th></th>
<th>95% Confidence Interval for Mean</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upper Bound</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic</td>
<td>2.1273</td>
<td>.47</td>
<td>7.94</td>
</tr>
<tr>
<td>Operational</td>
<td>1.9031</td>
<td>.01</td>
<td>7.94</td>
</tr>
<tr>
<td>Total</td>
<td>2.7565</td>
<td>.01</td>
<td>21.27</td>
</tr>
</tbody>
</table>

Outputs of D2M-Wizard and process for each of the generated models

This section has three subsections in it. The outputs of the first iteration of the D2M-Wizard, the outputs of the final data-cleaning iteration, and graphical representations of the two models.
Outputs of D2M-Wizard (cycle 0)

As depicted in Figure 37, the D2M-Wizard provides several output files each time a researcher executes it. Two output files of interest are the “suggested ngram” list and the “possible acronym” list. A summary of the sizes of these two output files, per model, is depicted in Table 12 and Figure 44. The variation in the sizes of two files is not a research question of interest, as they are both dependent on the number of input files fed into the D2M-process. The information below is illustrative of what a researcher could expect to see if they need to build a research center or project specific thesaurus from scratch by starting with these files. As I had access to the CASOS thesaurus as the basis of the D2M project, I focused my thesaurus generation effort on a DoD-specific model and supplemental per-model level thesauri.

<table>
<thead>
<tr>
<th>Model Level</th>
<th>Suggested ngrams</th>
<th>Possible Acronyms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>174,821</td>
<td>12,273</td>
</tr>
<tr>
<td>Operational</td>
<td>207,687</td>
<td>13,192</td>
</tr>
</tbody>
</table>

Table 12: Size of D2M-Wizard generated “suggested ngrams” list and “possible acronyms” list

![Figure 44 Size of D2M-Wizard generated ngram list and possible acronym list](image)

<table>
<thead>
<tr>
<th>Model Level</th>
<th>Singletons</th>
<th>N-Grams (multiple words==a single concept)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>30,205</td>
<td>29,122</td>
</tr>
<tr>
<td>Operational</td>
<td>29,821</td>
<td>33,299</td>
</tr>
</tbody>
</table>

Table 13: Quantities of D2M-Wizard generated ngram and singleton concepts draw from the union of generated ‘concept lists’
As depicted in Figure 37, other D2M-Wizard output files are the ‘concept list,’ the ‘finalThesaurus,’ and the metanetwork of inter-nodal and intra-nodal links. The ‘concept list’ is a list of D2M-identified concepts from the input corpus with the D2M generated suggested ontological category and without any attempt at mapping concepts to other concepts. Fundamentally, it’s a direct transcription of the concepts in the corpus reflecting only pre-processing modifications the researcher chooses to execute.

The third and fourth tables below summarize the link and node/entities information, Table 14 and Table 15 respectively, in the first metanetwork created by the D2M-Wizard. The D2M-Wizard creates links between nodes when those nodes co-occur within a sliding window of words within an input text. This co-occurrence network becomes the metanetwork of the input text with the link weight representing the number of co-occurrences between any two linked nodes. By creating a union of all the metanetworks for each corpus, the D2M-Wizard creates a metanetwork from each corpus representing the two models.

<table>
<thead>
<tr>
<th>Network</th>
<th>Links</th>
<th>Density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>8,760,073</td>
<td>0.00313213</td>
</tr>
<tr>
<td>Operational</td>
<td>5,983,375</td>
<td>0.00300365</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>raw counts</th>
<th>agent</th>
<th>belief</th>
<th>event</th>
<th>knowledge</th>
<th>location</th>
<th>organization</th>
<th>resource</th>
<th>role</th>
<th>task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>58,861</td>
<td>3,365</td>
<td>247</td>
<td>83</td>
<td>2,447</td>
<td>489</td>
<td>1,917</td>
<td>2856</td>
<td>281</td>
</tr>
<tr>
<td>Operational</td>
<td>63,120</td>
<td>4,696</td>
<td>36</td>
<td>23</td>
<td>2,434</td>
<td>557</td>
<td>2,660</td>
<td>3630</td>
<td>3</td>
</tr>
</tbody>
</table>

% of raw count

| Strategic | 5.72% | 0.42% | 0.14% | 4.16% | 0.83% | 3.26% | 4.85% | 0.48% | 2.34% |
| Operational| 7.44% | 0.06% | 0.04% | 3.86% | 0.88% | 4.21% | 5.75% | 0.00% | 1.33% |
The output file ‘finalThesaurus’ serves as a mapping of concepts to concepts, as well as concepts to ontological categories. The ‘finalThesaurus’ file is typically a conglomeration of thesauri that starts with, in this dissertation, the CASOS Standard Thesaurus. The information in Table 16 illustrates what a researcher could expect to see after a single iteration of the D2M-process using a research center thesaurus. Of particular note is the column labeled “Unknown” where many automation generated concepts have no ontological category. For each of the models, over 70% of concepts would, ideally, need deletion or an assigned category in the thesaurus. Depending on the corpus and research question(s), other researchers will have different distributions of entities per category per corpus, as well as different sized thesauri. The concepts captured in the D2M-process entries in Table 16 are reflective of applying the CASOS thesauri and dissertation thesauri, to the input sets.
### Table 16: ‘Concept list’ entities per ontological category for D2M cycle 0

<table>
<thead>
<tr>
<th>Category</th>
<th>Raw Counts</th>
<th>#Delete</th>
<th>agent</th>
<th>attribute</th>
<th>belief</th>
<th>event</th>
<th>knowledge</th>
<th>location</th>
<th>organization</th>
<th>resource</th>
<th>role</th>
<th>task</th>
<th>time</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>58,861</td>
<td>51</td>
<td>3,365</td>
<td>1,238</td>
<td>247</td>
<td>83</td>
<td>2,447</td>
<td>489</td>
<td>1,917</td>
<td>2,856</td>
<td>281</td>
<td>1,376</td>
<td>250</td>
<td>44,259</td>
</tr>
<tr>
<td>% of raw count</td>
<td>0.09%</td>
<td>5.72%</td>
<td>2.10%</td>
<td>0.42%</td>
<td>0.14%</td>
<td>4.16%</td>
<td>0.83%</td>
<td>3.26%</td>
<td>4.85%</td>
<td>0.48%</td>
<td>2.34%</td>
<td>0.42%</td>
<td>75.19%</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>63,120</td>
<td>66</td>
<td>4,696</td>
<td>744</td>
<td>36</td>
<td>23</td>
<td>2,434</td>
<td>557</td>
<td>2,660</td>
<td>3,630</td>
<td>3</td>
<td>840</td>
<td>427</td>
<td>47,004</td>
</tr>
<tr>
<td>% of raw count</td>
<td>0.10%</td>
<td>7.44%</td>
<td>1.18%</td>
<td>0.06%</td>
<td>0.04%</td>
<td>3.86%</td>
<td>0.88%</td>
<td>4.21%</td>
<td>5.75%</td>
<td>0.00%</td>
<td>1.33%</td>
<td>0.68%</td>
<td>74.47%</td>
<td></td>
</tr>
</tbody>
</table>

### Table 17: ‘finalThesaurus’ entities per ontological category D2M cycle 0

<table>
<thead>
<tr>
<th>Category</th>
<th>Raw Counts</th>
<th>#Delete</th>
<th>agent</th>
<th>attribute</th>
<th>belief</th>
<th>event</th>
<th>knowledge</th>
<th>location</th>
<th>organization</th>
<th>resource</th>
<th>role</th>
<th>task</th>
<th>time</th>
<th>Blank, None, Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>518,696</td>
<td>5,520</td>
<td>124,975</td>
<td>5,086</td>
<td>1,246</td>
<td>5,810</td>
<td>76,166</td>
<td>138,107</td>
<td>82,221</td>
<td>43,345</td>
<td>82</td>
<td>8,581</td>
<td>4,572</td>
<td>22,985</td>
</tr>
<tr>
<td>% of raw count</td>
<td>1.06%</td>
<td>24.09%</td>
<td>0.98%</td>
<td>0.24%</td>
<td>1.12%</td>
<td>14.68%</td>
<td>26.63%</td>
<td>15.85%</td>
<td>8.36%</td>
<td>0.02%</td>
<td>1.65%</td>
<td>0.88%</td>
<td>4.43%</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>541,574</td>
<td>5,581</td>
<td>126,733</td>
<td>6,658</td>
<td>1,245</td>
<td>5,897</td>
<td>80,304</td>
<td>138,440</td>
<td>88,165</td>
<td>46,818</td>
<td>82</td>
<td>8,725</td>
<td>6,276</td>
<td>26,650</td>
</tr>
<tr>
<td>% of raw count</td>
<td>1.03%</td>
<td>23.40%</td>
<td>1.23%</td>
<td>0.23%</td>
<td>1.09%</td>
<td>14.83%</td>
<td>25.56%</td>
<td>16.28%</td>
<td>8.64%</td>
<td>0.02%</td>
<td>1.61%</td>
<td>1.16%</td>
<td>4.92%</td>
<td></td>
</tr>
</tbody>
</table>
**Final outputs of D2M-process**

The D2M-process usually requires multiple rounds of cleaning in ORA™, thesaurus addition/modification, evaluation of Key Entities (see also Equation 12 on page 41) reports, and re-execution of D2M Scripts, all of which Figure 38 illustrate. Terminating the cycle of refinement is, at present, a researcher decision based on their question(s) of interest and the types of validation they desire to execute. For this dissertation, and in support of ‘validation in parts,’ I used 20 cycles for the operational model, and 12 cycles for strategic model. Termination conditions I used are shown in below.

<table>
<thead>
<tr>
<th>Table 18: Three (3) terminating conditions for D2M-process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Key Entity Reports for each node type include no obvious ‘wrong’ entities (e.g., an ‘Agent’ entity in the ‘Resource’ top-10 list) nor entities that could be meaningfully merged.</td>
</tr>
<tr>
<td>2. Subreports for Key Entities, for the top 50 entries, included no obvious ‘wrong’ entities nor entities that could be meaningfully merged.</td>
</tr>
<tr>
<td>3. Organization models included principal organizational and agent structures typical of military organizations (e.g., Commander, principle staff of A/G/S -1 through A/G/S7, and where appropriate, G8 and G9, as well as AOC-internal structures). Identifiable through tabular data in key entity reports as well as graphical renditions of the metanetworks.</td>
</tr>
</tbody>
</table>

Tabular Summary per Model

The data depicted in Table 19 reflects the composition of the final versions of each of the three supplemental thesauri the dissertation uses: DoD-wide, Strategic Model, and Operational Model. These supplemental thesauri are deliverables of the dissertation and may reduce the time between starting and conducting useful for future DoD organization modelers. These thesauri are independent of the wizard generated thesauri shown in Table 17—the entries in Table 17 reflect combination of the CASOS research center’s master thesaurus and the concepts in the three sets. The substantial differences in each of these thesauri are easily understood by recalling that the majority of the DoD-Master thesaurus is from the preceding work modeling and simulating resilient command and control with multiple USAF Air Operations Centers (Lanham, Morgan, et al., 2011b, 2011d). This origin, and the further de-scoping of the dissertation’s operational model, explains the very small model-specific thesauri and the large number of ‘delete’ actions in the operational thesaurus. It was unexpected, though in retrospect not surprising, that the strategic thesaurus is very different. The size of the thesaurus was significantly larger, with each of the ontological categories exhibiting larger changes than either of the other thesaurus. There is
insufficient data across multiple domains and variations within domains to determine if these differences are within the band of normal or not.

Table 20 reflects the composition of the meta-models of each of the models. A brief discussion of the differences between the starting meta-models (see also Table 15) and the final models is in order. Each of the metanetworks in cycle-0 had an unknown category that the final models do not contain. The cycle of editing these models and reviewing them for appropriate scope allowed varying levels of reductions in model size, with consequential reductions in processing times within the static assessment as well as eventual simulation. There could be research questions embedded in the apparent difference in the quantity of ‘agents’ in the Strategic corpus compared to the operational corpus. This could reflect an emphasis on the heads of various organizations responsibilities, but it remains an area of future work to determine if there is meaning behind the change in categorical distributions.

Table 21 provides a very brief view of the sizes and densities of each of these metanetworks. The changes in the nature of each corpus (e.g., its intended audience, orientation to particular levels-of-war) and the varying thesauri created an unexpected variation in the quantities of links and densities. Both models, at round zero (0) had approximately the same density (0.003). I had initially expected that the final densities of the models would align with the final node counts—the highest density would belong to the strategic model with the lowest in the operational model. This remains a question deferred to future work however.
### Table 19: Count per Ontological Category for each of the four final per-model thesauri (cycle 12 and higher)

<table>
<thead>
<tr>
<th>Thesaurus</th>
<th>Raw Counts</th>
<th>#Delete</th>
<th>agent</th>
<th>attribute</th>
<th>belief</th>
<th>event</th>
<th>knowledge</th>
<th>location</th>
<th>organization</th>
<th>resource</th>
<th>role</th>
<th>task</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD-Master</td>
<td>63,586</td>
<td>3,841</td>
<td>3,841</td>
<td>1,719</td>
<td>1,682</td>
<td>1,056</td>
<td>12,333</td>
<td>2,833</td>
<td>10,584</td>
<td>10,056</td>
<td>2,950</td>
<td>12,482</td>
<td>131</td>
</tr>
<tr>
<td></td>
<td>6.17%</td>
<td>6.04%</td>
<td>2.70%</td>
<td>2.65%</td>
<td>1.66%</td>
<td>19.40%</td>
<td>4.46%</td>
<td>16.65%</td>
<td>15.81%</td>
<td>4.63%</td>
<td>19.63%</td>
<td>0.21%</td>
<td></td>
</tr>
<tr>
<td>Strategic</td>
<td>23,083</td>
<td>3,065</td>
<td>1,196</td>
<td>270</td>
<td>492</td>
<td>2,667</td>
<td>1,326</td>
<td>4,219</td>
<td>3,830</td>
<td>426</td>
<td>5,421</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>13.28%</td>
<td>5.18%</td>
<td>0.72%</td>
<td>1.17%</td>
<td>2.13%</td>
<td>11.55%</td>
<td>5.74%</td>
<td>18.28%</td>
<td>16.59%</td>
<td>1.85%</td>
<td>23.48%</td>
<td>0.02%</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>1,611</td>
<td>1,525</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>26</td>
<td>2</td>
<td>46</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of raw count</td>
<td>94.66%</td>
<td>0.25%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1.61%</td>
<td>0.12%</td>
<td>2.86%</td>
<td>0.31%</td>
<td>0.06%</td>
<td>0.12%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 20: Metanetwork entities per ontological category (cycle 12 and higher)

<table>
<thead>
<tr>
<th>Thesaurus</th>
<th>Raw Counts</th>
<th>agent</th>
<th>belief</th>
<th>event</th>
<th>knowledge</th>
<th>location</th>
<th>organization</th>
<th>resource</th>
<th>role</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>25,190</td>
<td>3,308</td>
<td>469</td>
<td>317</td>
<td>4,216</td>
<td>1,379</td>
<td>3,696</td>
<td>5,456</td>
<td>694</td>
<td>5,619</td>
</tr>
<tr>
<td>% of raw count</td>
<td>13.13</td>
<td>1.86%</td>
<td>1.26%</td>
<td>16.74%</td>
<td>5.47</td>
<td>14.67%</td>
<td>21.66%</td>
<td>2.76%</td>
<td>22.31%</td>
<td></td>
</tr>
<tr>
<td>Operational</td>
<td>17,635</td>
<td>1,481</td>
<td>443</td>
<td>168</td>
<td>4,195</td>
<td>850</td>
<td>4,142</td>
<td>2,358</td>
<td>788</td>
<td>3,210</td>
</tr>
<tr>
<td>% of raw count</td>
<td>8.40%</td>
<td>2.51%</td>
<td>0.95%</td>
<td>23.79%</td>
<td>4.82%</td>
<td>23.49%</td>
<td>13.37%</td>
<td>4.47%</td>
<td>18.20%</td>
<td></td>
</tr>
</tbody>
</table>

### Table 21: Metanetwork descriptives (cycle 12 and higher)

<table>
<thead>
<tr>
<th>Thesaurus</th>
<th>networks</th>
<th>links</th>
<th>density</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>45</td>
<td>1,695,229</td>
<td>0.00534342</td>
</tr>
<tr>
<td>Operational</td>
<td>45</td>
<td>1,546,983</td>
<td>0.00994922</td>
</tr>
</tbody>
</table>

### Table 22: N-grams vs. Singletons, Acronyms vs. nonacronyms (cycle 12 and higher)

<table>
<thead>
<tr>
<th>Element</th>
<th>Quantity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>N-grams</td>
<td>42,920</td>
<td>62.7%</td>
</tr>
<tr>
<td>Singletons</td>
<td>25,563</td>
<td>37.3%</td>
</tr>
<tr>
<td>Acronyms</td>
<td>4,664</td>
<td>6.8%</td>
</tr>
<tr>
<td>Non-Acronyms</td>
<td>63,819</td>
<td>93.2%</td>
</tr>
</tbody>
</table>
Table 22 allows a comparison between the cycle-0 list of possible ngrams and acronyms list to the contents of the final DoD-Master Thesaurus. The final thesaurus has more ngrams than cycle-0 estimated, and fewer acronyms. The cause(s) of the variation is not clear, though I suspect the acronym-to-ngram conversion in the thesaurus is partly responsible—I deliberately converted many acronyms to their ngrams, as well as included their ngrams as part of the thesaurus. Nor is it entirely clear if the cause(s) of the variation are probative to the research question at hand.

Table 23 depicts a component of the output model that the D2M model process is not yet capable of generating. The specific nature of this research question requires the ability to differentiate agents and resources that a contested cyber environment can affect. There is no direct mechanism in the text-mining process to differentiate such agents and resources. Instead, through a completely manual process, I reviewed the lists of agents and resources for the various models and created ‘attributes’ that would allow me to differentiate IT agents from non-IT agents. Examples of IT agents are computer systems that generate or receive electronic messages, with or without direct human intervention. IT agents also typically perform some level of storage and processing on those messages as well as support habitual interaction by humans in the performance of their human-tasks. Examples of such systems include: Email, Blue Force Tracker, web-portals, databases, RSS servers, and other such systems. A set of encoding heuristics is shown in Table 61 for continued use or clarification.

Clearly, many IT systems susceptible to contested cyber environments do not fit into that somewhat amorphously defined category of IT agents above. As a simplification mechanism, I have an additional category that I have labeled IT resources. These are information technology dependent or enabled capabilities that are not typically considered message generating or passing, storing or manipulating. There is some level of risk in how and where I drew boundaries for these two groups, as neither label adequately expresses nuances or multi-purposed systems—are radars resources and their processing units IT agents, is the entire radar system (e.g., emitter, receiver, processing and communications units) an IT agent? The necessity of applying arbitrary selection criteria for binning these systems and systems-of-systems is a reflection of the gaps in the research space I discuss in the related literature. It may be infeasible to create a contested cyber environment against radar emitters and receivers (ignoring the debates about whether electronic jamming or
spoofing, electronic warfare is a form of cyber operations), though should an adversary act against processing or communications components, it is feasible to create effects through the loss of confidentiality, integrity, or availability.

The distribution of IT agents and IT resources within the models, as well as the master attributes list in Table 23 does provoke some thoughts: of specifically named and mentioned agents in the sets, over 20% are named or otherwise specific IT systems. This substantial fraction of agents is in line with the quantity of popular media stories and concerns by USG officials that the DoD is susceptible to contested cyber environments. Clearly, simple mentions of systems in doctrine and other documents does not necessarily connote their place or importance within organizations’ ability to execute their missions—it does however provide one more quantitative, not subjective, data point in mission assurance assessments. What I found somewhat more surprising is the smaller percentage of resources that fell into the IT resource bin. At just over 5% of the total number of resources, is there room for making a, possibly naive, assertion that such a small percentage of assets should never be cause for concerns about ‘Cyber Pearl Harbors’ and ‘existential threats?’ There is certainly room for such an assertion, but like IT agents, such infrequent references in doctrine may not indicate their actual importance within organizations. The inability of simple counting of references to establish importance to organizations is yet another reflection of the gaps in existing research.

Table 23: IT related agents and resources in all three generated models (cycle 12 and higher)

<table>
<thead>
<tr>
<th></th>
<th>Agents (IT &amp; Non-IT)</th>
<th>IT agents</th>
<th>Resources (IT &amp; Non-IT)</th>
<th>IT resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoD-Master Attributes List</td>
<td>3,303</td>
<td>852</td>
<td>10,056</td>
<td>578</td>
</tr>
<tr>
<td>% of node type</td>
<td>22.18%</td>
<td></td>
<td></td>
<td>5.75%</td>
</tr>
<tr>
<td>Strategic Model</td>
<td>3303</td>
<td>242</td>
<td>5451</td>
<td>161</td>
</tr>
<tr>
<td>% of node type</td>
<td>7.33%</td>
<td></td>
<td></td>
<td>2.95%</td>
</tr>
<tr>
<td>Operational Model</td>
<td>1,386</td>
<td>373</td>
<td>2,342</td>
<td>124</td>
</tr>
<tr>
<td>% of node type</td>
<td>27.21%</td>
<td></td>
<td></td>
<td>5.29%</td>
</tr>
</tbody>
</table>

Moving from tabular summary to one of the strengths of ORA™ as a network analytics tool, I will now review the terminating Key Entities reports for each of the three models.
Final Key Entities Report – Operational

The Key Agent’s visualization for the operational model, with the agent node set remaining the aggregation of human agents and IT systems identified in the source documents is in Figure 46. The figure shows ‘Commander’ ranks in the top three in 90% of agent-related measures with the more specific ‘Combined Joint Force Air Component Commander’ (CJFACC) being the next highest ranked agent, tied with ‘adversary,’ at 56%. Unsurprisingly, Joint and Air Force doctrinal documents place great emphasis on the commander, and his/her place in the organization. Like Army documents and the Tactical model, valence is absent in this Air Force-centric model.

To further assess the validity of the top-three agent recurring report, I expanded the visualization to those agents that consistently appear in the top 20 of their respective measures. This is shown in Figure 47. In this expanded view, the nonspecific agent ‘Commander’ remains in the top most position, with the CJFACC now tied. There remains some ambiguity in the source text about the Joint Staff—this technique is not yet capable of differentiate whether a given reference is to the Joint Staff supporting the Joint Chiefs of Staff in Washington, D.C., or the staff of a joint command. Of potential note is the absence of a specific agent, other than commanders, usually associated with the cyber domain. There is however, a number of IT systems in this expanded view, to include the generalized common operating picture (COP), the ISR Tracking System, and the generic ‘information system (info_sys).’
Like the Tactical model, it is necessary to disaggregate the IT agents from the agent node class to gain a better understanding of the relative importance of the human and IT agents within the metanetwork. This disaggregation allows for a finer grained understanding of the structural characters of two different agent types. The disaggregated human recurring agents visualization is below in Figure 48. In it, the corpus clearly reveals a high level of emphasis (and high variability within measures) on commanders and various specific organizational leaders. The paucity of the agents displayed is indicative of the variability of the human agents’ rankings within each measure.

To overcome the small number of agents revealed above, I again expanded the window of recurrence to the top 20 finishers in each measure. With this expanded view, in Figure 49, the human agent population continues its lack of cyber oriented agents and
remains operational focused on Air Force operations at the operational level of war. It did expand to include a number of other specific military leaders at various levels. One feasible interpretation of this emphasis on leadership is the Air Force’s doctrine places the emphasis of mission assurance on commanders and military leaders and not cyber specific agents or roles. If this interpretation is accurate, the Air Force is choosing a different path to technical assurance than the Army has chosen.

For the disaggregated IT agents population, when limited to the top three finishers per measure, the information revealed in Figure 50, demonstrates variability among the doctrine documents about which IT systems are important enough to be specifically mentioned. The Global Command and Control System (GCCS), in all its Service-specific incarnations, is the most frequently mentioned IT system, but even then is only in the top three of measures 50% of the time.

Extending the window of analysis to the IT agents that are in the top 20 of each measure, reveals a piece of information that I had previously thought of as anecdotal only—units rely on internet relay chat (IRC) far more than usually given credit for. Variability is still fairly high, though GCCS is now joined by the generic COP, the Joint Operations Planning and Execution System (JOPES), as well as the theater battle management core system (TBMCS) as frequently mentioned IT systems. This report provides evidence that SME-based assessments of the importance of TBMCS, JOPES, and GCCS are supported with quantitative analysis.
At the organization level, Joint and USAF doctrine are highly variable for the organizations that are consistently and frequently mentioned. This is shown in Figure 52 where only the generic organization of ‘staff’ rises to the 80% mark for consistent importance in network measures. Not surprising in their presence, though their low values remain at odds with professional experience, are the staff divisions for Intelligence and Operations. I had expected these organizations to be prominent in this kind of report and graph. A possible source for the discrepancy is the common view frame of authors—if they all simply ‘know’ that operations and intelligence divisions are important, they do not write such apparently self-evident facts. It’s unclear that commanders at the operational level of war would be necessarily surprised—if there was such a common reaction, the discrepancy could help Services adjust their writing styles.
Expanding the threshold for visualization from the top 3 recurring organizations to the top 20, Figure 53 below, allows us to see the variability does not appreciably change, though the number and types of units certainly does. At this threshold, the top entries do not change in their inclusion or relative order with the exception of the operations divisions. There is certainly ambiguity over which level of joint staff operations this entity refers to—National J3, COCOM level J3, Joint Task Force J3, or Combined Joint Staff J3. The absence of the logistics community in this model is likely more a reflection of the corpus selection than a lack of institutional emphasis on logistics at the tactical levels. It is extremely unlikely that the Air Force is cavalier to the importance of their logistics trail to their ability to conduct operations.
The Operational Model Resources captured by the D2M process, below, and the
thesauri I applied yield only a four (4) entities that doctrine consistently cross the 25%
threshold. Like the tactical model, the aggregation of IT resource and non-IT resource in this
report is not terribly illuminating.

![Figure 54 Recurring Top Ranked Resources (top 3), Operational Model](image)

Expanding the window of analysis to the resources that appear in the top 20 of these
measures, Figure 55, does not yield any more coherent presentation of resources that are
specific enough to address and important enough to have organizations dedicate resources to
their improving their resilience. It is gratifying to see that networks and IT, both in generic
incarnations, are in this view of the data, though lower than professional experience would
lead me to expect.

![Figure 55 Recurring Top Ranked Resources (top 20), Operational Model](image)

When disaggregating IT resources from non-IT resources, the resource picture does
not become more meaningfully clear, though a review remains in order. Below, Figure 56,
depicts that there are only three (3) highly generic resources that rise to the top 3 even 10% of the time. The generalized resources of capabilities, systems, and personnel are insufficiently precise to drive assessments of mission assurance. This insufficiency is, possibly, a selection error. The result may be a function of the texts that comprise the evaluated corpus—a more corpus more precisely aligned with a specific organization may generate more meaningful results. Before making further judgments on the usefulness of this disaggregation and report, it’s time to review the top 20 results of each measure and the disaggregated IT resources generated in the D2M process.

In Figure 57, the same generic resources are at the top of the list, revealing they are in the top 20 of all the resource-related measures. This report and analysis though is equally nonrevelatory as the previous report. The doctrine, as the source of the data, is insufficiently verbose in the resources listed to support primary decisions about named resource importance. However, a metanetwork ontology’s strength is that one segment of a model may not have direct measurable significance, but that segment still exists within the structure of the overall evaluated model. This presence supports establishing face validity of the model, and potentially increases the acceptability of results from other portions of the structure and model. In other words, importance to the network may very well be in the positioning within the multi-node system, not simply existence of a single node class.

![Figure 56 Recurring Top Ranked Non-IT resources (top 3), Operational Model](image-url)
The IT resources graphs, in contrast to the non-IT resources graphs, reveal entities that are recognizable and reasonable to Combatant Command and US Air Force cyber familiar and aware personnel. Figure 58 reflects the importance that popular media places on communications capabilities (of all types with no specificity) as well as networks (generally) and computer networks. There is some ambiguity whether ‘networks’ and ‘computer_networks’ refer to the same concept or if there was some meaningful contextual difference in the corpus. Given previous reports on the relative importance of the intelligence divisions of this level of warfare, it is gratifying to discern the intelligence network (JWICS) being present in the report as well. It is interesting to note that the named unclassified and secret networks (NIPRNet and SIPRNet) are not apparent while JWICS is present. The tactical model also reflected this absence of NIPRNet and SIPRNet.
Expanding the analysis window to the top 20 finishers in each resource related measure generates Figure 59. In this chart the generic communications capabilities remain high in the report, and JWICS rises even higher. The World Wide Web is a relabeling of NIPRNet (not technically accurate but a reasonable abstraction) and has near parity with JWICS in this view. Interestingly, a specific-to-coalition environments network (CENTRIX) appears in this view, which corresponds to the national trend of operating in coalition environments. There is also a more apparent importance of satellite based capabilities such as Global Positioning System (GPS), communications, and the generic ‘space_capabilities’—a frequent euphemism for classified capabilities).

This operational-level section has demonstrated that the second of the three stopping conditions listed in Table 18 is met. Later in this chapter, we will see the evidence of meeting the third stopping condition for the operational model.

![Figure 59 Recurring Top Ranked IT resources (top 20), Operational Model](image)

Final Key Entities Report – Strategic

This section is similar to the previous operational model just discussed, the Key Entities Reports review of D2M output for the Operational models. It provides a snapshot of the complete quantitative and visual representation of key entities for interesting node sets. I, again, provide the complete key entities reports (all 238 pages) on my home page at [http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support](http://www.andrew.cmu.edu/user/mlanham/nonpeer.shtml#dissertation_support).
The Key Agent’s visualization for the strategic model, with the agent node set remaining the aggregation of human agents and IT systems identified in the source documents is in Figure 60. The figure shows ‘CDR-Commander,’ ‘Combatant Commander’ (Combatant Command Commander), and ‘SECDEF’ (Secretary of Defense) rank in the top three (3) in 100%, 86% and 84%, respectively, in twenty-nine (29) different measures. The generic ‘info_sys’ and JOPES (Joint Operational Planning and Execution System) are the only two IT specific agents that make it into this summary of the measures. Like the other two models, it is not surprising that Joint doctrinal documents place great emphasis on commanders in general while specifically calling out Combatant Command Commanders, and the Secretary of Defense. In the US military chain of command, the SECDEF is second only to the President for civilian leadership. Unsurprisingly, at least in the aggregated collection of human and IT agents, named and specific IT systems are not frequently in the doctrine in the top three places of the various measures. One explanation of this could be it reduces the probability of needing to republish doctrine for each new technology change. Another plausible, and not mutually exclusive explanation is that doctrine is supposed to be a guideline and framework—not a specified collection of how and when to use what tools to accomplish tasks. It was surprising how low the CJCS ranked, the almost complete absence of supporting staff positions, and the National Security Council and its role in US military operations.

![Figure 60 Recurring Top Ranked Agents (top 3), Strategic Model](image)

Using the same process as the other two models, the expanded visualization of those agents that consistently appear in the top 20 of their respective measures is shown in Figure 61. In this expanded view, the top three agents are identical, though their relative position has
changed with the SECDEF rising to the second place. The Geographic Combatant Commanders have risen to the 3rd place in this chart, revealing there is ambiguity in doctrine when authors refer to Combatant Commanders—variants include Combatant Commanders, the Geographical Combatant Commanders, or the Functional Combatant Commanders, or some combination? Also in this view, we begin to see the presence of IT specific systems, though their labels remain generalized (e.g., info_sys, databases, and common operating picture) with one specifically named system: Global Air Mobility Support System (GAMES).

Disaggregating the IT agents from the human agents yields another example of differentiating the relative importance of the two agent types. The disaggregated human recurring agents visualization is below in Figure 62. The disparity between the three (3) most important agents and the remainder was not expected and is not reflective of what professional experience would have suggested.

Figure 61 Recurring Top Ranked Agents (top 20), Strategic Model
For further exploration of the top ranked human agents, I again expanded the window of recurrence to the top 20 finishers in each measure. With this expanded view, in Figure 63, the human agent population has a much broader swath of responsibilities than the generic ‘commander’, the SECDEF, and the Combatant Commanders. With this expanded view, we start seeing the inter-relatedness of the logistics community (USTRANSCOM), the intelligence community (IC) in the form of the Director of National Intelligence (DNI), the individual military departments and the component commands those departments furnish. Though it may have been reasonable to prune the model to reflect only those organizations in Figure 40, I decided that for the initial stopping point of face validity to allow the intermingled data/entities to remain where the corpus placed them.
For the disaggregated IT agents population, the information revealed Figure 64, demonstrates the near universal prominence in doctrine held by JOPES. Generic databases are a near second with all other specific IT agents in the top three of the measures 30% of the time or less. With such variability, the continued expansion of the analysis window to the top twenty (20) finishers in each measure remains apropos.

Figure 64 Recurring Top Ranked IT agents (top 3), Strategic Model

Figure 65 reveals that this level of granularity there is much less variability between the named IT systems. The number of supporting interests has also grown from those whose primary consumer are ‘commanders’ to those supporting interests and elements such as intelligence, supply operations, and provide/operate/maintenance of network/telecommunication networks.

Figure 65 Recurring Top Ranked IT agents (top 20), Strategic Model
At the organization level, the strategic model reveals that doctrine writers have broadened their scope of interest to include numerous organizations inside the Department of Defense as well as other governmental agencies (OGA), as shown in Figure 66. The top ranked organizations form the top tier of the nation’s war fighting commands—the combatant commands, their respective service component commands, and their respective higher headquarters. The rankings of the other displayed organizations, at less than 10% of measures, remain too varied to do more than speculate about meaning or causation.

Expanding the threshold for visualization from the top 3 recurring organizations to the top 20 allows us to see the robustness of the model. The variability in depicted results is smaller than previously as well as reflecting a wider variety of organizations that strategic doctrine writers frequently mention. This result is reflective of the actual complexity of organizations that come together to wage our nation’s wars: its more than infantry, tanks, and airplanes fighting in and over muddy fields. From the D2M process, the model includes not only the principal strategic military formations, but also elements of other government entities (e.g., CDC), Field Agencies and Agencies, and the ubiquitous Special Operations Forces (SOF).

The Strategic Model’s resources, Figure 68 below, depict several nonspecific resources but most interestingly, one very specific IT based resource: Joint World Wide Intelligence Communications System (JWICS). The consistently and prominent presence of this IT resource is indicative of the value of both intelligence at the Strategic level (that is
data converted to information and assessed by analysts) and the movement of intelligence across the various consumers within the USG. Unmentioned, but essential to realize, is that the Department of Defense owns and operates very little of its own network infrastructure—it relies on commercial public and private operators for communications links around the globe. JWICS, though cryptographically separated from other traffic on these links, is still fundamentally reliant on commercial providers for the bulk of its bandwidth and availability.

Expanding the window of analysis to the resources that appear in the top 20, Error! Reference source not found., of these measures does not meaningfully clarify the importance of any particular IT resource. The top ranking forces and capabilities are
generalized labels for resources available to the DoD, but not clearly useful for a resilience assessment. The over-all ranking of JWICS drops, while the importance of other resources enter the assessment window.

![Figure 69 Recurring Top Ranked Resources (top 20), Strategic Model](image)

When disaggregating IT resources from nonIT resources, Figure 70, the resource picture does not become more meaningfully clear. The items listed as appearing zero (0) percent of the time across the measures, are in alphabetical order from the ranks of entities in the same numerical category—meaning there are only six (6) entities that appear in the top three (3) of the resource-oriented measures. Like the merged resource view depicted above, these entities are too generalized for meaningful resilience assessment and planning.

The expanded view of the top twenty (20) finishers per measure does not yield any more clarity. This result, somewhat consistent across all three of these models, suggests that doctrine is potentially inadequate to perform rapid resource enumeration. It is more likely that organizations’ documents about their standard operating procedures (SOPs) within each of their war fighting functions would be a richer enumeration source.
The IT resources graphs, Figure 72 and Figure 73, reveal entities that are recognizable and reasonable to a Joint cyber familiar and aware member of DoD. The generic AIS is reflective of the pervasiveness of IT within the department. JWICS remains, as indicated in the aggregated view, consistently mentioned in the top twenty (20) finishers of each resource-centric measure. The top 20 graph indicates that there are a significant number of systems deemed by various authors as important, but there is wide variability in the authors’ writings. The variability is potentially a good news review of available communications abilities. There is no single set of capabilities that form a critical IT hub that could disrupt the entire IT infrastructure of the DoD—at least not in doctrinal references.
This section has demonstrated that the second of the three stopping conditions listed in Table 18 is met for the Strategic model. The section later in this chapter entitled Final Graphical Renderings - Strategic provides the evidence of meeting the third stopping condition for the strategic model.

Final Graphical Renderings - Overview

Graph visualization is one of many ways to analyze the models in this dissertation, and is the third way (see also Table 18) to establish terminating conditions for the iterative D2M process. With 45+ networks per model, 18K+ nodes, and 1.4M+ nodes, visual representation of the entire metanetwork generally looks like a multi-colored ball of yarn—
sometimes visually striking but rarely fit to elucidate answers to questions. Instead, and as a
demonstration of organizational face validity, I present in the following figures
representations of the Organization x Organization networks for each of the three models.

A short discussion of what visual representations of networks and how ORA™ lets
researchers make visualization choices follows. Each network represents the co-occurrence
of each listed organization with other listed organizations. The numeric value for each link
represents the number of times the co-occurrence happened within the relevant corpus. For
example a link between a node labeled G_3 and G_2 indicates those two organizations co-
ocurred within a window of concepts in the relevant input corpus. A link weight of 20 for
such a link, as an arbitrary example, would indicate there were 20 such co-occurrences in the
relevant input corpus.

<table>
<thead>
<tr>
<th>Filter by link weights/values (per figure caption)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recursively hide isolated nodes and pendant nodes (nodes with only one connection to another node).</td>
</tr>
</tbody>
</table>
| Distance between nodes is a function of the link weight, with higher link weights representing
  stronger ties between nodes and hence visually closer together. |
| Nodes colored by a researcher imposed attribute defining approximate level of command within an
  Army tactical hierarchy, the Air Force operational hierarchy, and the strategic hierarchy. The colors
  are for high contrast and not for any doctrinal or semantic reflection of meaning, and are the first
  figure in each series of figures (i.e., ) |
| Removal of nodes from graph whose level-of-warfare is ambiguous (left blank) |

Final Graphical Renderings - Operational

The visualizations below are for the Operational model (Combatant Command to
Numbered Air Force). I include four visualizations of the same model, at three levels of link-
weight filtering and one filtered by the exogenously determined ‘level’ of command. Node
colors per ‘level’ of command are shown in the legend in Figure 74. Figure 75 is the version
with no filtering by link weight, and nodes with ambiguous levels of command colored in
translucent green. This is a fairly typical ball of yarn for such a large network and is
reflective of the challenges of rendering large numbers of meaningfully discrete objects.
Figure 76 however begins to reveal itself as closer to attaining face validity through its two
principal colors, purple for the combatant command, blue for the Air Force Service
Component (USAFCENT) and red and orange for various AOC elements. In this view, each
of the five (5) principle divisions of the AOC are visible, as well as the cross functional
teams and groups. In Figure 77, the model reveals the even stronger links with the filtering
set to 15 or higher, though it is still clearly dominated by the purple joint and semi-joint elements of the Combatant Command, the Joint Air Force Component, and other elements associated with cyber operations. Figure 78 depicts yet another level of filtering with links with edges 35 or higher depicted. Taken in isolation, a researcher might chose to interpret the filtered view of this weighted network as indicating that, from the 83 documents in the Operational Corpus, the emphasis tends to be on the joint and mostly joint elements of this set of organization.

Figure 74 Node color legend for Operational Organization x Organization visualizations

Figure 75 Operational Org x Org, no filtering by link weight

Figure 76 Operational Org x Org, filtering by level of warfare != blank (the level is unambiguously within scope, exogenously determined by researcher)

Figure 77 Operational Org x Org, filtering by link weight >= 15
Final Graphical Renderings - Strategic

The visualizations below are for the strategic model (NCA to STRATCOM, USCENTCOM, and USCYBERCOM). I include three versions of the same network, at three levels of link-weight filtering. Figure 75, with no filtering at all, is reflective of the challenges of rendering large numbers of meaningfully discrete objects. Filtering the displayed links and nodes by link weight, it’s apparent that a value of 15 (Figure 76) is insufficiently de-cluttered to make any reasonable SME assessment from visual inspection. By increasing the filter value to 35 (Figure 77) it is becoming more apparent that each of the intended primary organizations are present, though it’s indeterminate whether we have an excessive number of unnecessary organizations remaining in the model. , reflect choices any researcher can make as part of their model-refinement process, and when to stop such refinements. Via visual inspection, a SME can confirm relevant organizations and suborganizations are present, prune nodes not in scope to the research question, and in the opposite sense, decide to not prune nodes based on unanticipated but present links between nodes. I also included DoD elements associated with how the Department, in accordance with the National Strategy for Cyber, has decided it will conduct cyber operations at the strategic level.
Summary of D2M-process

This portion of the dissertation has discussed the origin of the data from which I have built three distinct models of portions of the US Department of Defense. Each model represents one simplified portion of the larger organization to assist demonstrating generalizability of the model building process. I have also presented a multi-step process as well as modifications of the CASOS D2M-process to support the model construction in this acronym and jargon filled domain. Finally, I have presented the numerical descriptives of each of the models derived from this text-to-model process. Recall that though one
deliverable of the dissertation is a process that can be followed by future researchers, and DoD modelers. Though it is a deliverable, the process is a means to an end. It is also a previously unavailable means that is significantly more rapid than any risk management framework compliance assessments in my professional experiences. This rapidity sets this process apart from other forms of organizational model construction. The process is also very accessible to un-augmented staff and supports the capturing and reflecting connections between and among nine (9) different node-types,

Changes to empirical models in support of Agent Based Modeling

I defer the discussion of the modifications to the empirical models to enable a near direct transition to the Construct simulation capability to the Agent Based Models and Modeling Chapter beginning on page 168.

Summary

In this chapter, I have discussed the methodology for collecting data I use in this dissertation. I introduced modified processes, modified and built new computing capabilities and tools to support the automation-aided construction of multimode and multiplex organizational models from documents about the modeled organizations. I have also postulated a possibly meaningful research area into the statistical distributions of the metanetwork ontology—though I defer execution of that research to future work for myself or other researchers. This rapid modeling approach represents one of the principal contributions of the dissertation to the field of mission assurance and organizational resilience to contested cyber environments.
Network Analytics and Resilience

Numerous standard social network analysis (SNA) measures for single node types, single-mode measures, can offer indicators of general resilience—though they suffer from being unable to capture context outside the modeled types. Likewise, if organizations do not conduct assessments over time with sufficient frequency, their indicators and assessments may fail to capture enough information for meaningful conclusions—or worse, woefully misinformed conclusions. It is entirely feasible that depending on the timing of pre- and post event data gathering (see also Figure 137), assessments would completely miss any indicators of performance-degrading events. Such ignorance in the presence of data is one of numerous justifications for dynamic network analysis (DNA)—that is the longitudinal application of SNA measures to a data set or organization. Longitudinal study of organizations and the events that affect those organizations can be resource intensive above and beyond the investment in time. Organizations must be able to identify their sense of ‘normal,’ identify when contested cyber environments begin and end, and identify the affect people, systems, processes, and other structural elements. Organizations must also be able to quantify those effects with a trustworthy methodology and meaningful effects. To these requirements, this chapter offers an exposition of theory applied to the domain of resilience to contested cyber environments. Exposition will be through application of quantitative SNA techniques to the models created in the Data-to-Model (D2M) process of the preceding chapter. The chapter also extends the SNA-domain of knowledge by providing a static measure of resilience as a function of near-isolation of agents, tasks, resources, and knowledge.

Harkening back to the dissertation work flow of Figure 35 and zooming in between the creation of the models and the augmentation leading to simulation, Figure 84 is another breadcrumb to assist the reader in knowing where this chapter fits in the workflow of the dissertation.
Resilience in what context?

Like (Pflanz, 2012; Pflanz & Levis, 2012) and revisiting Figure 2, a graph depicting the dynamic nature of resilience is useful to convey a more complete understanding.

In this Figure, there is a span of time from $t_0$ to $t_{\text{warmup}}$ that reflects the possible values of a Measure of Interest (MoI) prior to reaching a pre-contested-environment equilibrium. As noted by Pimm (1984), without equilibrium, resilience is indefinable. During the time of normal operations (MoI$\text{normal}$), the organization achieves some level of equilibrium with variance within
some acceptable tolerances. The figure also depicts the beginning of an attack ($t_{attack-start}$), or some other cause for a negative Confidentiality-Integrity-Availability (CIA) effect(s). While the attack is ongoing, the attack should be having some effect on the MoI, though it may not be consistent, statistically or operationally significant—absent an effect, there is no rational reason to expend resources to deal with the attack. As shown, there is an approximate stair step halfway through the attack...as just one of an infinite variety of possible impacts on the MoI (e.g. instantaneous drop, linear or step-wise linear drop, logarithmic drop, quadratic drop). At some point-in-time, the attack ends ($t_{attack-end}$), though there is no guarantee that the organization or its agents are aware of the specific end time—nor for that matter are they assured of being aware of a specific start time ($t_{attack-start}$). The chart above depicts a quiescent period after the attack and before ‘recovery’ begins ($t_{recovery}$), or before the MoI rises above the minimum performance reached as a consequence of the attack.

There is no requirement for recovery to start immediately, as the attack may have effects on the MoI that outlast the attack itself. It’s also important to note that there is a space between the minimum performance ($MoI_{min}$) for this MoI and a minimally acceptable threshold set, a priori, by one or more leaders of an organization of interest. This threshold may have been set, or may simply be a generalized statement by leadership akin to ‘no performance drop is acceptable!’ This picture does not depict a return to pre-attack levels for this MoI (at $t_{pre-attack}$ reached), indeed there is no universal requirement in definitions of resilience that such a return to pre-event levels occur, notwithstanding Bishop (2011). To be sure, in the happy situation shown above, the forecast is that the attack/attacker makes the organization better in this MoI than they might otherwise have become, with adaptation as a likely explanation.

In an attack, however, where the $MoI_{min}$ drops below $MoI_{min-acceptable}$, the MoI for the modeled organization would have low resilience, and potentially low-survivability. Such a situation would make recovery all the more daunting as first recovery efforts would be geared to re-gaining the $MoI_{min-acceptable}$ level of performance.

**Static resilience indicators**

Deciding which SNA-measures an organization can or should use to indicate resilience to cyber events is a fundamental task for any meaningful program of assessment and improvement. The decision may be existing-data driven—a measure with no supporting data is a theoretical
achievement un-anchored to any organizational reality. Of course, lack of data during the decision process can itself drive efforts to establish a recurring data collection mechanism that, ideally, imposes little differential loading on the organization itself. A brief example of SNA-measures and their applicability to the domain of cyber resilience follows.

When a resilience question relates to information or belief diffusion, a researcher could use changes in measured pre- and post event “communication speed” (Kathleen M. Carley, Pfeffer, Reminga, Storrick, & Columbus, 2012)—where the longest path length of the Agent-by-Agent (AA) network is an indicator of the speed that any arbitrary message can pass across the modeled network. This communication speed model is inappropriate to modeling specific technical-channel flows—for that goal a tool such as OMNet++ may be more applicable. However, realizing that humans frequently have more than one method of communicating with other humans, this measure abstracts away the details of channel selection, capacity, utilization, and congestion. In this abstracted manner, this model provides an indicator of possible changes to message passing speeds pre- and post event, and allows a quantitative assessment of the impact(s) to such message passing.

Negative changes in an organization’s Resource-by-Resource (RR) network (e.g., loss of links or nodes in the RR matrix), indicating possible loss of system-to-system communications links or unfulfilled inter-dependencies are another application of SNA to the myriad facets of resilience assessment and engineering. Not all changes are necessarily negative in their impacts. It is entirely feasible that the loss of access to one or more systems by one or more agents and their organizations may lead the organization to successful adaptive behavior. Where the behavior is deleterious to the desired organizational outcomes, leadership and assessors have succeeded in identifying mal-adaptive behavior as well. Before discussing further applications of SNA measures to cyber resilience assessments, it is appropriate to look at the results of measures calculations on the three models in the dissertation: tactical level; operational level; and strategic level.

This application of network analytics to organizational resilience is akin to the CARVER method of targeting used by the US military and some of its military allies. US Joint and Service doctrine discuss CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability) as a methodology to help quantify the inputs to the targeting decision.
processes—what resources, organizations, or people should the military apply force against, to what effect, and for how long should the effect last. With CARVER as a near analog, it’s an easy leap to using standard centrality measures (e.g., inDegree, outDegree, geodesic centrality (Freeman, 1977)) for agents and message-passing resources. These measures have other analogs in the idea of span-of-control (the number of direct-report subordinates a leader can effectively manage).

**Metanetwork resilience indicators**

Several metanetwork-based measures are also suggestive of potentially useful measures of interest. A partial list, primarily those contributing to the new measure ‘resilience’ is in Table 25, with a more complete list in Table 26.

Network measures, in particular the general network/organization measures shown below, would be infeasible without multimode networks. Calculations using matrix algebra support the creation of measures such congruence between knowledge and resources available and that needed for task completion. The same is true for the multimode assessment of cognitive demand (expanding past the effort humans expend to keep their social networks to the effort humans expend to maintain their social networks, manage their resources, and execute their tasks). Finally, Graham’s work on shared situation awareness (SSA) would be infeasible without the added information in a metanetwork representation of an organization.

ORA™, with over 170 measures, helps assess static resilience in the two models using immediate impact assessments or the following metrics applied to the metanetwork using entropic and targeted node removal. A sampling of those measures are below in Table 25.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Meaning from Carley (2002d) and ORA™ Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance as Accuracy</td>
<td>How accurately agents can perform their assigned tasks based on their access to knowledge and resources.</td>
</tr>
<tr>
<td>Communication Congruence</td>
<td>Measures to what extent the agents communicate when and only when it is needful to complete tasks. Perfect congruence requires a symmetric Agent x Agent network.</td>
</tr>
<tr>
<td>Knowledge Congruence</td>
<td>Across all agents, the knowledge that agents lack to do their assigned tasks expressed as a percentage of the total knowledge needed by all agents.</td>
</tr>
<tr>
<td>Key Node Identification</td>
<td>Using Key Entity reports</td>
</tr>
<tr>
<td>Shared Situation Awareness</td>
<td>A function of Eigen vector centrality, social</td>
</tr>
</tbody>
</table>
New and adjusted metanetwork resilience indicators

There are two sets of new measures of resilience under consideration. The first is a single measure that combines several existing measures. The second is a set of measures that provide over time assessment, and therefore requires over time data—in this dissertation generated through simulation and discussed in the next two chapters.

The first point-in-time measure is a multivariable function shown in (14). This is a multivariable function of normalized network access indices for knowledge, resources and tasks, organizational needs and the organizational waste. Access indices are reflections of near isolation, organizational needs reflects shortfalls in knowledge and resources needed to do tasks, and organizational waste represents knowledge supplied to tasks (via agents) that tasks do not need for their execution. The final three-part result is in (14), with the incremental steps to build to the equation shown in (15) through (35) along with additional definitions and explication for each component. Exogenous weighting factors, \( \alpha, \beta, \text{ and } \lambda \) are shown as well, though for this dissertation I set them to one (1) in the absent of evidence supporting other values. I have drawn and derived this measure from (Kathleen M. Carley & Pfeffer, 2012c; Kathleen M. Carley, Juergen Pfeffer, et al., 2012) with minor axial shifts.

\[
\text{Resilience} = \alpha \left( \frac{1}{1 + e^x} + \frac{1}{1 + e^y} + \frac{1}{1 + e^z} \right) + \beta \left( \frac{1}{1 + e^n_{\text{knowledge}}} + \frac{1}{1 + e^n_{\text{resource}}} \right) + \lambda \left( \frac{1}{1 + e^{-w_{\text{knowledge}}}} + \frac{1}{1 + e^{-w_{\text{resource}}}} \right)
\]

Equation 14 Structural resilience as a new metanetwork calculation
The three-part access index component, multiplied by $\alpha$, is a measure of near isolation for three node types: knowledge, tasks, and resources. Near isolation is another way of referring to a single point of failure (SPOF) — albeit possibly irrelevant to specific questions of interest. For the agent node set, (15) shows how to compute the knowledge access index. In English, for each agent, a possibly empty set of knowledge entities ($\mathbb{K}$) exists of knowledge to which only the one agent has access. Additionally, the agent (ego) with access connects to only one other agent (alter)—the ego is a pendant with respect to all alters.

\[
\forall A, \mathbb{K}_a = \{ k \mid A \mathbb{K}(i,k) \wedge (\sum A \mathbb{K}(:,k) = 1) \wedge (\sum A \mathbb{A}(i,:) = 1) \}\]

Equation 15 Access index as reflection of criticality through near isolation (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

The intuition is that the effect of this type of SPOF corresponds to an inverse sigmoid function (aka S-curve), such that low numbers of SPOFs correspond to high levels of structural resilience. I normalize the access index by the magnitude of its source node set. I then segment the result into 12 bins—12 bins allows the output curve to align with the Army’s (though not Air Force or Joint) color coding scheme for unit combat effectiveness. With normalized results of (15) ranging from [0, 1], the sigmoid function must shift to the right to reflect zero near isolates equate to the maximal output of the function ($x=0 \rightarrow f(x)=1$). The exponent of the sigmoid function is shown in (16) with the final sigmoid function shown in (17).

\[
\mathbb{K}'_a = \frac{\sum \mathbb{K}_a}{12} - 6 = \frac{12 \times \sum \mathbb{K}_a}{|\mathbb{K}|} - 6
\]

Equation 16 Normalized summation of a model’s knowledge access index, agents aggregated

\[
\text{Knowledge Access Component} = \frac{1}{1 + e^{\mathbb{K}'_a}}
\]

Equation 17 Knowledge access component sigmoid, right shifted six values, in 12 bins

---

6 The four (4)-color ‘Gumball’ method of representing unit effectiveness at a glance is green, amber, red, black. These colors correspond to combat capable/100%-85% strength, combat capable/70-84% strength, Combat Ineffective/50-69% strength, and requires reconstitution/<50% strength (Headquarters Department of the Army, 2010). In this color-coding scheme, a decrease in a measure of 30-50% corresponds with an organization in need of reconstitution/regeneration before receiving additional missions. Decreases of 15% or less correspond with no change in visual representation of the measure—the color code remains ‘green.’
Equation (17) depicts all types of agents aggregated into a single group. In this dissertation I disaggregated Agents (nominally humans or roles humans fill) and IT Agents (nominally computer-based systems or capabilities that process, store, manipulate transmit and receive data). To accommodate this disaggregation I modified (16) by summing the two ORA™-calculated Knowledge Access Indices before normalizing. This modification is shown in (18) with the consequent update to (17) reflected in (19).

\[
K'_{a+ita} = \frac{12 \times (\sum K_a + \sum K_{ita})}{|K|} - 6
\]

Equation 18 Normalized summation of a model’s knowledge access index, agents disaggregated

\[
KnowledgeAccessComponent = \frac{1}{1 + e^{K'_{a+ita}}}
\]

Equation 19 Knowledge access component sigmoid, right shifted six values, in 12 bins, agents disaggregated

Identical calculations then occur for tasks as shown in (20). Calculations for Resource Access Index had to accommodate the combinatoric effects of disaggregating IT resources from Resources as well as disaggregating Agents and IT Agents and is shown in (21).

\[
T'_{a+ita} = \frac{12 \times (\sum T_a + \sum T_{ita})}{2 \times |T|} - 6
\]

Equation 20 Normalized summation of a model’s task access index, agents disaggregated

\[
ResourceAccessIndex = \frac{12 \times (\sum R_a + \sum R_{ita} + \sum ITR_a + \sum ITR_{ita})}{2 \times |R + ITR|} - 6
\]

Equation 21 Normalized summation of a model’s resource and IT resource access index, agents disaggregated

The use of (19), (20), and (21) to build the combined access index component causes that component to look like (22) below.

\[
AccessIndexComponent = \alpha \left( \frac{1}{1 + e^{K'_{a+ita}}} + \frac{1}{1 + e^{T'_{a+ita}}} + \frac{1}{1 + e^{R'_{a+ita}}} \right)
\]

Equation 22 Access Index Component, adjusted for disaggregation of Agent and Resource node sets

---

7 ORA™ does not yet support direct calculation of task access index. To accomplish this, I recoded the ‘Task’ node set as a ‘Knowledge’ node set and re-executed the knowledge access index calculation report in ORA™.
A 2D projection of the sum of two of the above indices is below, with the addition of the third index left as an exercise for the reader. It is easy to discern that when there are no SPOFs, the highest score shown for two (2) indices is two (2). The Access Index Component is therefore a function with a range of [0, 3] with three (3) being the best possible score, representing no SPOFs for tasks, knowledge, or resources.

![Access Index Component (2 of 3, missing Task Access Index x 12 -6)](image)

Figure 86 2D projection of 3D rendering of two access indices

The next portion of building (14) is the calculation, at an organization level, of the knowledge and resource shortfalls. Within ORA™, the measures names are \textit{congruenceOrgTaskKnowledgeNeeds} and \textit{congruenceOrgTaskResourceNeeds}. \textit{congruenceOrgTaskKnowledgeNeeds} reveals “Across all tasks, the knowledge that tasks lack expressed as a percentage of the total knowledge needed by all tasks” (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). A value of zero (0) is an excellent result for both measures. Using the same number of bins as the access index calculations, I again right shift the curve six (6) values. I also translate the percentage to one of 12 bins as shown in (25) and then used as input into a standard sigmoid function shown in Figure 87. Figure 87 is a reduced form of the Access Index Component with only two (2) functions summed, causing a reduction in the range from [0,3] to [0, 2]. Zero (0) is indicative there are no tasks lacking knowledge of any variety.
Figure 87 Sigmoid function of Knowledge + Resource Needs Component, low input values best

\[ S_k = AT^T \times A^T K \] (23)

Equation 23 Tasks with needed knowledge via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ n_{knowledge} = \frac{\sum_{t=1}^{[T]} \sum_{k=1}^{[K]} KT'(t,k) \times (S_k(t,k) = 0)}{\sum KT} \] (24)

Equation 24 Percentage of knowledge not provided by agents assigned to tasks (Knowledge Needs) (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ \hat{n}_{knowledge} = (n_{knowledge} \times 12) - 6 \] (25)

Equation 25 Knowledge needs, right shifted 6 values, in 12 bins

\[ Needs_{KnowledgeResource} = \frac{1}{1 + e^{n_{knowledge}}} + \frac{1}{1 + e^{n_{source}}} \] (26)

Equation 26 Needs Component as sum of two sigmoid needs functions, right shifted 6 values, in 12 bins

Again, there are modifications to (26) necessary due to the disaggregation of agents and IT agents. To merge and normalize the \( n_{knowledge} \) value for agents and IT agents, it is necessary to unwind the percentage values of each, and recalculate a normalized value. This process is in (27).

\[ \hat{n}_{knowledge_{agent+itagent}} = 12 \times \left( \frac{n_{knowledge_{agent}} \times |T|}{2 \times |T|} + \frac{n_{knowledge_{itagent}} \times |T|}{2 \times |T|} \right) - 6 \] (27)

Equation 27 congruenceOrgTaskKnowledgeNeeds with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)
Equation 28 Tasks with needed resources via assigned agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ S_r = AT \times AR \]  

Equation 29 Percentage of resources not provided by agents assigned to tasks (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ n_{resource} = \frac{\sum_{i=1}^{[AT]} \sum_{r=1}^{[AR]} RT(t,r) \times (S_r(t,r) = 0)}{\sum RT} \]  

Equation 30 Resource needs, right shifted 6 values, in 12 bins

\[ n_{resource} = (n_{resource} \times 12) - 6 \]  

Equation 31 congruenceOrgTaskResourceNeeds with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ n_{resource} = 12 \times \left( \frac{n_{resource_{agent}} \times |R| + n_{resource_{agent}} \times |IR| + n_{resource_{agent}} \times |ITR| + n_{resource_{agent}} \times |ITR|}{2 \times |R + ITR|} \right) - 6 \]  

The measure congruenceOrgTaskKnowledgeWaste reveals “Across all tasks, the knowledge that agents have that are not required to do their assigned” (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). Intuitively, having extra knowledge within an organization is inefficient but potentially useful in some crisis or exigency. As such, this aspect of the resilience score uses an inverted sigmoid function, indicating that zero (0) waste is bad, and that superfluous knowledge or resources are good. Using the same number of bins as the access index calculations, I again right shift the curve six (6) values as well as translate the percentage to one of 12 bins as shown in (36) and used as input into Figure 88.
Figure 88 Sigmoid function of Knowledge + Resource Waste Component, high input values best

\[ w_{knowledge} = \frac{\sum_{k=1}^{n} S_k(t,k) \times \text{KT}(t,k)}{\sum_{k=1}^{n} S_k(t,k)} \] (32)

Equation 32 Percentage of knowledge not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ w'_{knowledge} = \left( w_{knowledge} \times 12 \right) + 6 \] (33)

Equation 33 Knowledge waste, right shifted 6 values, in 12 bins

Again, there are necessary modifications to (33) due to the disaggregation of agents and IT agents. To merge and normalize the \( w_{knowledge} \) value for agents and IT agents, it is necessary to unwind the percentage values of each, and recalculate a normalized value. This process is shown in (34).

\[ w'_{knowledge} = 12 \times \left( \frac{w_{knowledgeagent} \times |T| + w_{knowledgeinagent} \times |T|}{2 \times |T|} \right) + 6 \] (34)

Equation 34 congruenceOrgTaskKnowledgeWaste with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[ w_{resource} = \frac{\sum_{r=1}^{R} S_r(t,r) \times \text{RT}(t,r)}{\sum_{r=1}^{R} S_r(t,r)} \] (35)

Equation 35 Percentage of resources not used for tasks assigned to agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)
\[ w'_{\text{resource}} = (w_{\text{resource}} \times 12) + 6 \] (36)

Equation 36 Resource ‘Waste,’ right shifted 6 values, in 12 bins

The modifications to (36) due to the disaggregation of resources and IT resources follow the same pattern as the modification for \( w_{\text{knowledge}} \). With two disaggregations, IT Agents and IT resource, there are four (4) percentage values to unwind and renormalize This process is shown in (37).

\[
6 + 12 \times \left( \frac{w_{\text{resource}}_{\text{agent}} \times |R| + (w_{\text{resource}}_{\text{agent}} \times |R|) + (w_{\text{resource}}_{\text{agent}} \times |ITR|) + (w_{\text{resource}}_{\text{agent}} \times |ITR|)}{2 \times (|R| + |ITR|)} \right)
\] (37)

Equation 37 congruenceOrgTaskResourceNeeds with disaggregated agents and IT agents (Kathleen M. Carley, Juergen Pfeffer, et al., 2012)

\[
Waste_{\text{KnowledgeResource}} = \frac{1}{1 + e^{-W_{\text{knowledge}}}} + \frac{1}{1 + e^{-W_{\text{resource}}}}
\] (38)

Equation 38 Waste Component as sum of two sigmoid waste functions, right shifted 6 values, in 12 bins

A 2D projection of (14) is shown in Figure 89 as well as a surface mapping of the interaction between a single growth curve (i.e. a single waste value) and a single decay curve (e.g., a single access index value or a single needs value) in Figure 90. A more comprehensive (for output values) surface depiction is in Figure 91. All three of these figures depict that the ideal resilient organization should have no near isolates, maximal excess knowledge and resources (e.g., twice what is minimally necessary), and no needs. They also show that the least resilient organization is hyper-efficient in knowledge and resource distribution with no waste whatsoever. The least resilient organization also has the degenerate case that all tasks, resources, and knowledge are near isolates and accessible only through agents that are pendants. Finally the least resilient organization has every task short of necessary knowledge and resources.
Returning to (14), Figure 91 offers a more nuanced rendering of the interactions between the grouped outputs. Unlike previous graphs, I am rendering a sampling of the possible output values for each of the three components of (14). At the far right, high component scores each contribute to a high score for resilience. It is also read as there exists no, zero, unique knowledge/tasks/resources possessed by pendant agents. There are no knowledge or resource
shortages for any tasks, and there are twice as much knowledge in the organization as assigned tasks need. The opposite end of the graph, at the left, depicts a scenario where there is nothing but unique knowledge and resources possessed by pendants. There are shortages of knowledge and resources for every task, and there is no excess knowledge or resources of any kind in the organization. Such an organization scores a zero (0) in this resilience measure.

Figure 91 3D surface rendering of theoretical resilience scores, as function of access indices, wastes, and needs

Resilience indicators for strategic and operational models

We can assess network models of organizations in terms of their structural changes when a node or sets of links leave an organization. Picking the nodes to delete is of course one of challenges and which to pick depends on the task at hand—disruption of information flow or ensuring continued information flow? Breaking a network into segments with a single deletion or multiple deletions and under what constraints? To explore these questions, node-level measures help generate Key Entity reports, thereby reducing the possible deletion pool from the entire model to a more restricted set of nodes. Network-level measures then provide the pool of measures of interests (MoIs) that reflect the effects of IT agents and IT Resource node deletions. Potentially, we are also interested in the changes to node-level metrics for the nodes left behind as well—identifying shifts in node-level metrics for follow-on analysis or action. In light of the above, I present here a list of network measures, their base line values, and discussion points that
can serve as markers of resilience to contested cyber environments. It is likely, in future research, that additional network measures within ORA™ can add to the robustness of analysis and expand the scope of possible disrupting or negative events as well as to-be-developed measures.

Table 26: Dissertation Measures of Interest (MoI)

<table>
<thead>
<tr>
<th>Network Measure</th>
<th>Discussion and How/Why it is relevant to assessing resilience in a contested cyber environment$^8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resilience Score</td>
<td>The proposed newest measure seeks to quantify the vulnerability based on scarcity of access to resources, knowledge and tasks. The perception that an entity with few connections to the rest of the model could have significant effects through its absence runs counter to many more traditional modes of social network analysis. It does however mesh with the specialization of functions and roles within modern organizations with broad ranges of responsibilities.</td>
</tr>
<tr>
<td>Resilience Score</td>
<td>Across all agents, the amount of knowledge needed for completion of assigned tasks, expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values.</td>
</tr>
<tr>
<td>Resilience Score</td>
<td>Across all agents, the amount of knowledge possessed by agents not required by assigned tasks. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.</td>
</tr>
<tr>
<td>Resilience Score</td>
<td>Across all tasks, the amount of knowledge lacking to tasks expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values.</td>
</tr>
<tr>
<td>Resilience Score</td>
<td>Across all tasks, the amount of excess knowledge to tasks expressed as a percentage of total knowledge needed. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.</td>
</tr>
</tbody>
</table>

The remainder of the network-level measures are in alphabetical order:

| Characteristic Path Length | For each node set, the average path length across all linked nodes in that set. Most relevant to linked human and IT agents that manipulate and process information while performing tasks. The shorter the path, the faster information may flow. Path lengths not perturbed by node deletions indicate resilience to path disruptions. Excessively high path lengths can, though out of scope for this work, indicate room for pruning communications links within an organization. |
| Congruence, Organization Agent Knowledge Needs | Like knowledge needs, but with respect to resources. Clearly low needs values are more appropriate for organizations than high values. |
| Congruence, Organization Agent Knowledge Wastes | Like knowledge wastes, but with respect to resources. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values. |
| Congruence, Organization Agent Resource Needs | Across all agents, the amount of knowledge needed for completion of assigned tasks, expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values. |
| Congruence, Organization Agent Resource Wastes | Across all agents, the amount of knowledge possessed by agents not required by assigned tasks. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values. |
| Congruence, Organization Task Knowledge Needs | Across all tasks, the amount of knowledge lacking to tasks expressed as a percentage of total knowledge needed. Clearly low needs values are more appropriate for organizations than high values. |
| Congruence, Organization Task Knowledge Wastes | Across all tasks, the amount of excess knowledge to tasks expressed as a percentage of total knowledge needed. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values. |

$^8$ Unless otherwise noted, definitions and explanations for these measures are verbatim from (Kathleen M. Carley, Juergen Pfeffer, et al., 2012). Discussion of applicability to the dissertation is original work by the author.
Table 26: Dissertation Measures of Interest (MoI)

<table>
<thead>
<tr>
<th>Network Measure</th>
<th>Discussion and How/Why it is relevant to assessing resilience in a contested cyber environment*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Congruence, Organization Task Resource Needs</td>
<td>Like task knowledge needs, but with respect to resources. Clearly low needs values are more appropriate for organizations than high values.</td>
</tr>
<tr>
<td>Congruence, Organization Task Resource Wastes</td>
<td>Like task knowledge wastes, but with respect to resources. Wastes, when not substitutable for other knowledge, represent expenditure of cognitive resources by agents that they might otherwise use for the benefit of the organization. Lower values will generally be preferable over high values.</td>
</tr>
<tr>
<td>Congruence, Social Technical</td>
<td>The match between the coordination requirements established by the dependencies among tasks and the actual coordination activities carried out by the engineers. In other words, the concept of congruence has two components. First, the coordination needs determined by the technical dimension of the socio-technical system and, secondly, the coordination activities carried out by the organization representing the social dimension (Cataldo, Herbsleb, &amp; Carley, 2008).</td>
</tr>
<tr>
<td>Density, Clustering Coefficient</td>
<td>The average of nodes’ clustering coefficient. The higher the value the more like a small world network—the more the network supports local information diffusion as well as a decentralized infrastructure.</td>
</tr>
<tr>
<td>Diffusion</td>
<td>Computes the degree to which something could be easily diffused (spread) throughout the network. This is based on the distance between nodes—inferred when latitude/longitude data is not available for the Location node set. A large diffusion value means that nodes are close to each other, and a smaller diffusion value means that nodes are farther apart.</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>The proportion of nodes disconnected from the network, though not completely isolated. The more fragments in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole.</td>
</tr>
<tr>
<td>Isolate Count</td>
<td>The number of isolates in a model. The more isolates in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole.</td>
</tr>
<tr>
<td>Overall Complexity</td>
<td>The density of the metanetwork as a whole. Denser network have more links between nodes than less dense networks, usually indicating higher resilience to node removal.</td>
</tr>
<tr>
<td>Performance as Accuracy</td>
<td>Measures how accurately agents can perform their tasks based on the agent’s access to knowledge required of the tasks.</td>
</tr>
<tr>
<td>Social Density</td>
<td>Density of the Agent x Agent network.</td>
</tr>
<tr>
<td>Speed</td>
<td>The inverse of the average shortest path length between two arbitrary nodes.</td>
</tr>
<tr>
<td>Shared Situation Awareness (Aggregated)</td>
<td>This is usually a node-level and dyad-level measure. However, when aggregated across all agents in a model, it can provide a view of the mean and distribution of the value.</td>
</tr>
</tbody>
</table>
Baseline resilience measures of interest (MoI)

**MoI 1: Baseline resilience score**

The descriptive statistics below in Table 27 reflect the baseline for each of the D2M models. In this research, the strategic model earned a higher resilience score than the operational. There is insufficient data to speculate on the causation of why the resilience score ordering mimics the ordering of the levels of war. The data below does however indicate that strategic organizations have substantial knowledge and resources at their general disposal for reacting to negative events—though the measure does not attempt to assess how difficult any adaptations may be.

<table>
<thead>
<tr>
<th>Model</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Statistic</td>
<td>Statistic</td>
<td>Statistic</td>
</tr>
<tr>
<td>Strategic</td>
<td>1</td>
<td>5.581919</td>
<td>5.581919</td>
<td>5.5819196</td>
</tr>
<tr>
<td>Operational</td>
<td>1</td>
<td>5.087243</td>
<td>5.087243</td>
<td>5.0872437</td>
</tr>
</tbody>
</table>

**MoI 2: Baseline characteristic path length resilience score (agent, IT Agent, IT Resource)**

ORA™ also labels characteristic path length as averageDistance. The strategic and operational models, as shown in Table 28 have an above average score based on (Kathleen M. Carley & Kim, 2008). This indicates that as modeled, these organizations have a smaller average value for links between arbitrary agents (and IT resources). This score is reflective of the organization’s ability to pass information quickly between agents.

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Statistic</td>
<td>Statistic</td>
<td>Statistic</td>
</tr>
<tr>
<td>strategic</td>
<td>averageDistance_agent</td>
<td>1</td>
<td>4.352554</td>
<td>4.352554</td>
<td>4.35255400</td>
</tr>
<tr>
<td></td>
<td>averageDistance_IT Agent</td>
<td>1</td>
<td>5.461147</td>
<td>5.461147</td>
<td>5.46114700</td>
</tr>
<tr>
<td></td>
<td>averageDistance_IT Resource</td>
<td>1</td>
<td>3.489093</td>
<td>3.489093</td>
<td>3.48909300</td>
</tr>
<tr>
<td>operational</td>
<td>averageDistance_agent</td>
<td>1</td>
<td>5.198773</td>
<td>5.198773</td>
<td>5.19877300</td>
</tr>
<tr>
<td></td>
<td>averageDistance_IT Agent</td>
<td>1</td>
<td>9.842969</td>
<td>9.842969</td>
<td>9.84296900</td>
</tr>
<tr>
<td></td>
<td>averageDistance_IT Resource</td>
<td>1</td>
<td>4.212481</td>
<td>4.212481</td>
<td>4.21248100</td>
</tr>
</tbody>
</table>
**MoI 3: Baseline Congruence, Organization Agent (and IT Agent) Knowledge Needs score**

The strategic model is ahead of the operational model for the IT Agents, but behind the operational model for Agents. For both models, agents are less well off than their electronic peers. The scores for both models indicate that the organizations have significant room for improvement—alternatively it indicates authors of documents about the organizations should be more robust in describing the links between people, technology, and tasks.

Table 29: Descriptive Statistics for D2M Congruence, Organization, Agent Knowledge Needs

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgAgentKnowledgeNeeds_task</td>
<td>1</td>
<td>.2422910</td>
<td>.2422910</td>
<td>.242291000</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentKnowledgeNeeds_task</td>
<td>1</td>
<td>.5885547</td>
<td>.5885547</td>
<td>.588554700</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgAgentKnowledgeNeeds_task</td>
<td>1</td>
<td>.2787664</td>
<td>.2787664</td>
<td>.278766400</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentKnowledgeNeeds_task</td>
<td>1</td>
<td>.4187375</td>
<td>.4187375</td>
<td>.418737500</td>
</tr>
</tbody>
</table>

**MoI 4: Baseline Congruence, Organization Agent (and IT Agent) Knowledge Wastes score**

These scores indicate that agents, IT agents, and roles in the doctrine-defined models have very little knowledge considered ‘waste.’ Waste in this context is knowledge with one or more links to agents, but there is no task that needs the knowledge to which the agents have links. In the context of (14), this corresponds with an output in the waste component of nearly zero (0), also indicating very little resilience to the loss of access to knowledge in the organization.

Table 30: Descriptive Statistics for D2M Congruence, Organization, Agent Knowledge Waste

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgITAgentKnowledgeWaste_task</td>
<td>1</td>
<td>.0443308</td>
<td>.0443308</td>
<td>.044330780</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentKnowledgeWaste_task</td>
<td>1</td>
<td>.0140131</td>
<td>.0140131</td>
<td>.014013100</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgITAgentKnowledgeWaste_task</td>
<td>1</td>
<td>.0409634</td>
<td>.0409634</td>
<td>.040963360</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentKnowledgeWaste_task</td>
<td>1</td>
<td>.0275715</td>
<td>.0275715</td>
<td>.027571470</td>
</tr>
</tbody>
</table>

**MoI 5: Baseline Congruence, Organization Agent (and IT Agent) Resource (and IT Resource) Needs score**

This MoI contributes to one-third (1/3) of (14) in the needs component of that function. It reflects, across the agents in a network-based model of an organization, the percentage of tasks that lack required resources. The lack of resources does not assure failure of a task, but it does decrease the probability of successful and satisfactory completion. Unlike in MoI 3: Baseline
Congruence, Organization Agent (and IT Agent) Knowledge Needs score, the strategic model is in second place, behind the operational model in each disaggregated measure. Figure 92 depicts the same information in scatter plot form.

Table 31: Descriptive Statistics for D2M Congruence, Organization, [Agent | IT Agent] [Resource | IT Resource] Needs, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgAgentResourceNeeds_task</td>
<td>1</td>
<td>.1925941</td>
<td>.1925941</td>
<td>.192594100</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentResourceNeeds_task</td>
<td>1</td>
<td>.4864685</td>
<td>.4864685</td>
<td>.486468500</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentITResourceNeeds_task</td>
<td>1</td>
<td>.2038859</td>
<td>.2038859</td>
<td>.203885900</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentITResourceNeeds_task</td>
<td>1</td>
<td>.4391244</td>
<td>.4391244</td>
<td>.439124400</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgAgentResourceNeeds_task</td>
<td>1</td>
<td>.5028715</td>
<td>.5028715</td>
<td>.502871500</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentResourceNeeds_task</td>
<td>1</td>
<td>.6678281</td>
<td>.6678281</td>
<td>.667828100</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentITResourceNeeds_task</td>
<td>1</td>
<td>.9963437</td>
<td>.9963437</td>
<td>.996343700</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentITResourceNeeds_task</td>
<td>1</td>
<td>.5575537</td>
<td>.5575537</td>
<td>.557553700</td>
</tr>
</tbody>
</table>
**MoI 6: Baseline Congruence, Organization Agent Resource Wastes score**

This MoI contributes to one-third (1/3) of (14) in the waste component of that function. Figure 93 above, and Table 32 below, reflect the information for this MoI. This MoI, across the agents in a network-based model of an organization, is the percentage of tasks that have access to resources not explicitly required by tasks. The excess resources do not assure an organization of resource substitution or transfer, but they could conceivably increase the probability of successful and satisfactory completion in the event of loss of original resources. The operational model has the highest scores for this MoI with the strategic model barely half as good. The Supply Chain management domain of research would likely assert these low scores reflect a desirable allocation of resources—but with little to no excess resources to support reallocation, leaders have less decision and execution space to operate in.

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgAgentResourceWaste_task</td>
<td>1</td>
<td>.0227923</td>
<td>.0227923</td>
<td>.0227923</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentResourceWaste_task</td>
<td>1</td>
<td>.0991865</td>
<td>.0991865</td>
<td>.0991864</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentITResourceWaste_task</td>
<td>1</td>
<td>.0137338</td>
<td>.0137338</td>
<td>.0137337</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentITResourceWaste_task</td>
<td>1</td>
<td>.0416444</td>
<td>.0416444</td>
<td>.0416444</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentResourceWaste_task</td>
<td>1</td>
<td>.0516288</td>
<td>.0516288</td>
<td>.0516287</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentResourceWaste_task</td>
<td>1</td>
<td>.0709751</td>
<td>.0709751</td>
<td>.0709750</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgAgentITResourceWaste_task</td>
<td>1</td>
<td>.9989119</td>
<td>.9989119</td>
<td>.9989119</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgITAgentITResourceWaste_task</td>
<td>1</td>
<td>.2638718</td>
<td>.2638718</td>
<td>.2638718</td>
</tr>
</tbody>
</table>

**MoI 7: Baseline Congruence, Organization Task Knowledge Needs score**

From the task perspective, this measure reveals a mixed message for each of the D2M models. The operational model has the least variance between the two varieties of this measure, while the strategic model has the least needs across all the tasks. This measure suggests the strategic organizations modeled are better positioned for completing their tasks as they have fewer knowledge gaps. Fewer knowledge gaps generally correlate to higher rates of task completion as well as higher accuracy for those tasks.
Table 33: Descriptive Statistics for D2M Congruence, Organization, Task Knowledge Needs, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgTaskKnowledgeNeeds_agent</td>
<td>1</td>
<td>.1067627</td>
<td>.1067627</td>
<td>.1067627</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskKnowledgeNeeds_itagent</td>
<td>1</td>
<td>.3208613</td>
<td>.3208613</td>
<td>.3208613</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgTaskKnowledgeNeeds_agent</td>
<td>1</td>
<td>.2940585</td>
<td>.2940585</td>
<td>.2940585</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskKnowledgeNeeds_itagent</td>
<td>1</td>
<td>.2127802</td>
<td>.2127802</td>
<td>.2127802</td>
</tr>
</tbody>
</table>

MoI 8: Baseline Congruence, Organization Task Knowledge Wastes score

From the task perspective, there is an over abundance of knowledge in the models. The D2M models’ scores are congruent with what I expected of values in the range of 20-30%. The table below, and Figure 95 above indicate that the strategic model has very low variability between the two varieties but as an organization has a higher waste score than the operational model.
Table 34: Descriptive Statistics for D2M Congruence, Organization, Task Knowledge Waste

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgTaskKnowledgeWaste_agent</td>
<td>1</td>
<td>3109356</td>
<td>3109356</td>
<td>3109356</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskKnowledgeWaste_itagent</td>
<td>1</td>
<td>3117439</td>
<td>3117439</td>
<td>3117439</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgTaskKnowledgeWaste_agent</td>
<td>1</td>
<td>1960738</td>
<td>1960738</td>
<td>1960738</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskKnowledgeWaste_itagent</td>
<td>1</td>
<td>2271573</td>
<td>2271573</td>
<td>2271573</td>
</tr>
</tbody>
</table>

**MoI 9: Baseline Congruence, Organization Task Resource (and IT Resource) Needs score**

Like MOI 8, from the task perspective, this measure reveals a mixed message for the two models. The strategic model has the least variance for the four combinations of this measure. For the strategic model, the IT agents were worse off than regular agents in their needs. This alignment of tasks and resources for the strategic model, and the low starting value for this score, supports a higher resilience score than organizations with large shortages of resources. Figure 96 on the next page and Table 35 below reflect the data.

Table 35: Descriptive Statistics for D2M Congruence, Organization, [Agent | IT Agent] [Resource | IT Resource] Waste, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgTaskResourceNeeds_agent</td>
<td>1</td>
<td>.1042690</td>
<td>.1042690</td>
<td>.1042690</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskResourceNeeds_itagent</td>
<td>1</td>
<td>.2544663</td>
<td>.2544663</td>
<td>.2544663</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceNeeds_agent</td>
<td>1</td>
<td>.1094033</td>
<td>.1094033</td>
<td>.1094033</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceNeeds_itagent</td>
<td>1</td>
<td>.2706257</td>
<td>.2706257</td>
<td>.2706257</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgTaskResourceNeeds_agent</td>
<td>1</td>
<td>.4005018</td>
<td>.4005018</td>
<td>.4005018</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskResourceNeeds_itagent</td>
<td>1</td>
<td>.3523277</td>
<td>.3523277</td>
<td>.3523277</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceNeeds_agent</td>
<td>1</td>
<td>.9986320</td>
<td>.9986320</td>
<td>.9986320</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceNeeds_itagent</td>
<td>1</td>
<td>.0415371</td>
<td>.0415371</td>
<td>.0415371</td>
</tr>
</tbody>
</table>

**MoI 10: Baseline Congruence, Organization Task Resource Wastes score**

Unlike MoI 8 and 9, from the task perspective, this measure has a very coherent message for the strategic model compared to the mixed messages for the operational model. Table 36 and Figure 97, below, illustrate the strategic model, like MoI 9, has the least variance for the four combinations of this measure. For the strategic model, it has the least amount of waste, or excess resources for all the tasks in the model. The operational model had all four varieties of this measure above 30%.
Table 36: Descriptive Statistics for D2M Congruence, Organization, Task [Resource | IT Resource] Waste, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>congruenceOrgTaskResourceWaste_agent</td>
<td>1</td>
<td>.2333035</td>
<td>.2333035</td>
<td>.233303500</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskResourceWaste_itagent</td>
<td>1</td>
<td>.2731924</td>
<td>.2731924</td>
<td>.273192400</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceWaste_agent</td>
<td>1</td>
<td>.2663376</td>
<td>.2663376</td>
<td>.266337600</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceWaste_itagent</td>
<td>1</td>
<td>.2696142</td>
<td>.2696142</td>
<td>.269614200</td>
</tr>
<tr>
<td>operational</td>
<td>congruenceOrgTaskResourceWaste_agent</td>
<td>1</td>
<td>.3698346</td>
<td>.3698346</td>
<td>.369834600</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskResourceWaste_itagent</td>
<td>1</td>
<td>.3228272</td>
<td>.3228272</td>
<td>.322827200</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceWaste_agent</td>
<td>1</td>
<td>.9999931</td>
<td>.9999931</td>
<td>.999993100</td>
</tr>
<tr>
<td></td>
<td>congruenceOrgTaskITResourceWaste_itagent</td>
<td>1</td>
<td>.8789737</td>
<td>.8789737</td>
<td>.878973700</td>
</tr>
</tbody>
</table>

**MoI 11: Baseline Congruence, Social Technical score**

On a scale of [0,1], inclusive, this score indicates poor alignment between the assignment of tasks and the social connections needed to gain knowledge to execute those tasks for both models. I had not expected such low scores with these models. An initial hypothesis for why this score would be so low is that doctrinal documents rarely enumerate which particular people use...
which particular capabilities and systems to accomplish which particular tasks. The low scores suggest that additional work is necessary to establish how to get the score more congruent with professional opinion in the organizations themselves. It is unlikely that the leaders of the strategic and operational organizations would agree that there is such low alignment between their people and the technology their people need to accomplish their tasks.

Table 37: Descriptive Statistics for D2M Congruence, Social Technical

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>socialTechnicalCongruence_agent_task</td>
<td>1</td>
<td>.01065395</td>
<td>.10653950</td>
<td>.0106539500</td>
</tr>
<tr>
<td></td>
<td>socialTechnicalCongruence_task_itagent</td>
<td>1</td>
<td>.006576661</td>
<td>.06576661</td>
<td>.00657666100</td>
</tr>
<tr>
<td>operational</td>
<td>socialTechnicalCongruence_agent_task</td>
<td>1</td>
<td>.00364293</td>
<td>.00364293</td>
<td>.0036429330</td>
</tr>
<tr>
<td></td>
<td>socialTechnicalCongruence_task_itagent</td>
<td>1</td>
<td>.006184001</td>
<td>.06184001</td>
<td>.0618400100</td>
</tr>
</tbody>
</table>

**MoI 12: Baseline Density, Clustering Coefficient score**

This is a [0,1] scaled-measure, reflected in Table 39 and Figure 99 that assists a leader in learning how similar an organization is to a small-world network. Social network science circles have studied small-world networks and know the networks have very well defined characteristic Plans. One such prominent characteristic is the speed with which such networks of people can pass messages to each other. Given how the military often perceives of itself as a hierarchical organization, I expected these scores to be fairly low. It was somewhat surprising that IT agents and resources were as high as they were. Also surprising was that the strategic model was four times closer to being a small world model than the operational model. I do not have a working hypothesis for the disparity in scores between the two models and defer to future work hypothesizing about the differences.

Table 38: Descriptive Statistics for D2M Density, Clustering Coefficient

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>clusteringCoefficient_agent</td>
<td>1</td>
<td>.21368170</td>
<td>.21368170</td>
<td>.2136817000</td>
</tr>
<tr>
<td></td>
<td>clusteringCoefficient_itagent</td>
<td>1</td>
<td>.227304300</td>
<td>.227304300</td>
<td>.22730430000</td>
</tr>
<tr>
<td></td>
<td>clusteringCoefficient_itresource</td>
<td>1</td>
<td>.408167600</td>
<td>.408167600</td>
<td>.40816760000</td>
</tr>
<tr>
<td>operational</td>
<td>clusteringCoefficient_agent</td>
<td>1</td>
<td>.05838165</td>
<td>.05838165</td>
<td>.0583816500</td>
</tr>
<tr>
<td></td>
<td>clusteringCoefficient_itagent</td>
<td>1</td>
<td>.245274800</td>
<td>.245274800</td>
<td>.24527480000</td>
</tr>
<tr>
<td></td>
<td>clusteringCoefficient_itresource</td>
<td>1</td>
<td>.255845000</td>
<td>.255845000</td>
<td>.25584500000</td>
</tr>
</tbody>
</table>
MoI 13: Baseline Diffusion score

Computes the degree to which a network of agents can easily diffuse (spread) something throughout the network. Figure 99 and Table 39 visually depict the diffusion values for both modes. A diffusion value of 1 means that nodes are close to each other. Diffusion, in and of itself, has limited use to leaders attempting to assess their resiliency to adverse events such as contested cyber environments. However, it is a fast measure to calculate, and changes in the measure can support over-time assessment as well as forecasting. For both models, the IT resources seem better positioned for fast message propagation, which would be congruent with expectations of automated message passing.

Table 39: Descriptive Statistics for D2M Diffusion, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>diffusion_agent</td>
<td>1</td>
<td>2393415</td>
<td>2393415</td>
<td>239341500</td>
</tr>
<tr>
<td></td>
<td>diffusion_itagent</td>
<td>1</td>
<td>10742080</td>
<td>10742080</td>
<td>1074208000</td>
</tr>
<tr>
<td></td>
<td>diffusion_itresource</td>
<td>1</td>
<td>6412405</td>
<td>6412405</td>
<td>641240500</td>
</tr>
<tr>
<td></td>
<td>diffusion_agent</td>
<td>1</td>
<td>0312542</td>
<td>0312542</td>
<td>031254200</td>
</tr>
<tr>
<td></td>
<td>diffusion_itagent</td>
<td>1</td>
<td>15454540</td>
<td>15454540</td>
<td>1545454000</td>
</tr>
<tr>
<td></td>
<td>diffusion_itresource</td>
<td>1</td>
<td>3475332</td>
<td>3475332</td>
<td>347533200</td>
</tr>
</tbody>
</table>
**MoI 14: Baseline Fragmentation score**

The proportion of nodes disconnected from the network, though not completely isolated. The more fragments in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole. With this in mind, Figure 100 shows that IT resource fragmentation is the lowest of all three varieties of this measure. Both models’ agent varieties earn scores of .70 or higher, indicating a high level of agents not connected to the larger population. The same is true of their IT agents though less so for IT resources.

Table 40: Descriptive Statistics for D2M Fragmentation, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fragment_agent</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.76</td>
</tr>
<tr>
<td></td>
<td>fragmentation_itagent</td>
<td>1</td>
<td>8920292</td>
<td>8920292</td>
<td>.8920292</td>
</tr>
<tr>
<td></td>
<td>fragmentation_itresource</td>
<td>1</td>
<td>35813390</td>
<td>35813390</td>
<td>.35813390</td>
</tr>
<tr>
<td>operational</td>
<td>fragment_agent</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>.97</td>
</tr>
<tr>
<td></td>
<td>fragmentation_itagent</td>
<td>1</td>
<td>8448566</td>
<td>8448566</td>
<td>.8448566</td>
</tr>
<tr>
<td></td>
<td>fragmentation_itresource</td>
<td>1</td>
<td>65107780</td>
<td>65107780</td>
<td>.65107780</td>
</tr>
</tbody>
</table>

Figure 100 Fragmentation, Baseline

Figure 101 isolateCount [[IT]Agent|Resource], Baseline
**MoI 15: Baseline Isolate Count (Agents, IT agents, and IT resources) score**

This measure is a simple count of isolate nodes in a model. The more isolates in a model, the less likely the network is to diffusion information well, synchronize task execution, or otherwise perform as a purposeful whole. These agents did not get deleted during the cleaning processes, as I had chosen to only delete isolates in relation to the entire metanetwork. This means that so long as the agent was connected to any node of any node type, the cleaning process would not delete it. Overall, this is a mixed message across both models.

![Table 41: Descriptive Statistics for D2M Isolate Count, Baseline](image)

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>isolateCount_agent</td>
<td>1</td>
<td>201</td>
<td>201</td>
<td>201.00</td>
</tr>
<tr>
<td></td>
<td>isolateCount_itagent</td>
<td>1</td>
<td>205</td>
<td>205</td>
<td>205.00</td>
</tr>
<tr>
<td></td>
<td>isolateCount_itresource</td>
<td>1</td>
<td>299</td>
<td>299</td>
<td>299.00</td>
</tr>
</tbody>
</table>

**MoI 16: Baseline Overall Complexity score**

This value is the calculated density of the metanetwork as a whole. Denser networks have more links between nodes than less dense networks, usually indicating higher resilience to node removal among other characteristics. Density, in much the same way as diffusion, is very useful, easy to compute, and changes are easily observed during simulations. Significant changes in complexity are indicators of a change somewhere in the network, the nature of which a leader or researcher would need to exactly determine. In the resilience context, this measure proved less illuminating than expected.

![Table 42: Descriptive Statistics for D2M Complexity, Baseline](image)

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Complexity</td>
<td>1</td>
<td>0.002388317</td>
<td>0.002388317</td>
<td>0.002388317</td>
</tr>
<tr>
<td></td>
<td>Complexity</td>
<td>1</td>
<td>0.002537118</td>
<td>0.002537118</td>
<td>0.002537118</td>
</tr>
</tbody>
</table>

**MoI 17: Baseline Performance as Accuracy score**

Measures how accurately agents can perform their tasks based on the agent’s access to knowledge required of the tasks. This is a summary statistic that reflects the general probability that an organization will perform its tasks correctly. Low scores are not good, and while signaling to leaders a misalignment between people, tasks, resources, and knowledge, it does not
identify which particular tasks are more likely to be incorrect than others. Figure 102 and Table 43 depict the scores for the disaggregated collections of human and IT agents, as well as non-IT and IT resources. The operational model shows a higher variability among the groups than the strategic model, but both organizations have lower scores than I expected. These low scores detract from the face validity of the model with respect to this measure. The leaders of the organizations captured in the D2M process would surely disagree that their organizations are getting their tasks and missions done with less than 20% accuracy.

Table 43: Descriptive statistics for D2M performance as accuracy, baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Statistic</td>
<td></td>
<td>Statistic</td>
<td>Statistic</td>
<td>Statistic</td>
</tr>
<tr>
<td>strategic</td>
<td>performanceAsAccuracy_agent_resource</td>
<td>1</td>
<td>.198872000</td>
<td>.198872000</td>
<td>.198872000</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_agent_itresource</td>
<td>1</td>
<td>.184975500</td>
<td>.184975500</td>
<td>.184975500</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_itagent_resource</td>
<td>1</td>
<td>.027839</td>
<td>.027839</td>
<td>.02783935</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_itagent_itresource</td>
<td>1</td>
<td>.028977</td>
<td>.028977</td>
<td>.02897680</td>
</tr>
<tr>
<td>operational</td>
<td>performanceAsAccuracy_agent_resource</td>
<td>1</td>
<td>.041837840</td>
<td>.041837840</td>
<td>.0418378400</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_agent_itresource</td>
<td>1</td>
<td>.060753970</td>
<td>.060753970</td>
<td>.0607539700</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_itagent_resource</td>
<td>1</td>
<td>.028103</td>
<td>.028103</td>
<td>.02810312</td>
</tr>
<tr>
<td></td>
<td>performanceAsAccuracy_itagent_itresource</td>
<td>1</td>
<td>.037095</td>
<td>.037095</td>
<td>.03709463</td>
</tr>
</tbody>
</table>

Figure 102 performanceAsAccuracy, Baseline
**MoI 18: Baseline Social Density score**

At the core of every organization are its human resources. This measure captures the density of the known social network(s) as reflected in the links between agent nodes. This dissertation, as a result of disaggregating IT agents from agents, has two flavors of this measure per model. The data in Table 44 indicate a fairly low density for the organizations modeled. A working hypothesis is the doctrine documents need supplementing with more detailed internal SOPs to more closely reflect organizations’ self-perceptions.

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>density_agent</td>
<td>1</td>
<td>0.00646176</td>
<td>0.00646176</td>
<td>0.0064617550</td>
</tr>
<tr>
<td></td>
<td>density_agent_x_itagent</td>
<td>1</td>
<td>0.001520241</td>
<td>0.001520241</td>
<td>0.00152024100</td>
</tr>
<tr>
<td>operational</td>
<td>density_agent</td>
<td>1</td>
<td>0.00179914</td>
<td>0.00179914</td>
<td>0.0017991390</td>
</tr>
<tr>
<td></td>
<td>density_agent_x_itagent</td>
<td>1</td>
<td>0.001570701</td>
<td>0.001570701</td>
<td>0.00157070100</td>
</tr>
</tbody>
</table>

**MoI 19: Baseline Speed score**

The inverse of the average shortest path length between two arbitrary nodes. The data in Table 45 and Figure 104 both reveal that neither organization is near its theoretical maximum of 1.0. Not unexpectedly, the IT Resources have the highest scores with the human agents coming in noticeably slower.

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>averageSpeed_agent</td>
<td>1</td>
<td>0.2297502</td>
<td>0.2297502</td>
<td>0.229750200</td>
</tr>
<tr>
<td></td>
<td>averageSpeed_itagent</td>
<td>1</td>
<td>0.18311170</td>
<td>0.18311170</td>
<td>0.1831117000</td>
</tr>
<tr>
<td></td>
<td>averageSpeed_itresource</td>
<td>1</td>
<td>0.2866074</td>
<td>0.2866074</td>
<td>0.286607400</td>
</tr>
<tr>
<td>operational</td>
<td>averageSpeed_agent</td>
<td>1</td>
<td>0.1923531</td>
<td>0.1923531</td>
<td>0.192353100</td>
</tr>
<tr>
<td></td>
<td>averageSpeed_itagent</td>
<td>1</td>
<td>0.10159540</td>
<td>0.10159540</td>
<td>0.1015954000</td>
</tr>
<tr>
<td></td>
<td>averageSpeed_itresource</td>
<td>1</td>
<td>0.2373898</td>
<td>0.2373898</td>
<td>0.237389800</td>
</tr>
</tbody>
</table>
MoI 20: Baseline Shared Situation Awareness score
This is usually a node-level and dyad-level measure. However, when aggregated across all agents in a model, it can provide a view of the mean and distribution of the value. The rendition of this measure is shown below in Table 46 and above in Figure 105. These results were not congruent with expectations and certainly would not be in congruence’s with the perceptions of the leaders of the modeled organizations. A working hypothesis is that this measure may be ill suited to this form of model construction, as there are few indicators of actual location—and Graham et al. demonstrated that physical proximity was a large contributor to shared situation awareness {Graham, 2004 #7627}. 
### Table 46: Descriptive Statistics for D2M Shared Situation Awareness, Baseline

<table>
<thead>
<tr>
<th>Model</th>
<th>Measure</th>
<th>N</th>
<th>Minimum Statistic</th>
<th>Maximum Statistic</th>
<th>Mean Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategic</td>
<td>sharedSituationAwareness_agent</td>
<td>1</td>
<td>0.002326</td>
<td>0.002326</td>
<td>0.00232558</td>
</tr>
<tr>
<td></td>
<td>sharedSituationAwareness_itagent</td>
<td>1</td>
<td>0.001851852</td>
<td>0.001851852</td>
<td>0.00185185200</td>
</tr>
<tr>
<td>operational</td>
<td>sharedSituationAwareness_agent</td>
<td>1</td>
<td>0.002532</td>
<td>0.002532</td>
<td>0.00253165</td>
</tr>
<tr>
<td></td>
<td>sharedSituationAwareness_itagent</td>
<td>1</td>
<td>0.001524390</td>
<td>0.001524390</td>
<td>0.00152439000</td>
</tr>
</tbody>
</table>

### Entropic and Targeted Attacks

ORA™ is capable of performing two types of immediate impact assessments for models to gauge the variability of the resilience indicators in the previous section. The first type is through a replication analysis in which the researcher specifies how many random nodes from which data sets to remove and how many times to run the analysis. This is the entropic attack the heading of this section refers to. ORA™ randomly selects the nodes from among the nodeset (from a uniform distribution), removes the links to/from those deleted nodes, and then recalculates network measures. ORA™ generates the average deltas for the iterations performed.

Previous work (Kathleen M. Carley & Lanham, 2012) indicated that there were minimal impacts (all but one was less than 1% with the one measure changing only 3% from baseline) with random single entity removals. To confirm or refute those findings, I repeated the effort and set the number of entities to remove at one (1), four (4), and ten (10). I had not expected any changes in output measures averaged across multiple repetitions of arbitrary node removal. The results met my expectations—none of the measures above had any change when recorded across as few as 10 and as many as 1,000 repetitions. This result is most likely due to the sparseness of the various matrices as well as the long right-tailed distribution of link counts between nodes.

For exploratory purposes, and aligned with the Army’s Green/Amber/Red/Black color coding of combat capability, I conducted further experiments with random node removal of 15%, 30%, 50% and 75% losses. I also performed a round of deletions at a 90% level. Army doctrine color-codes a unit with up to 15% loss of combat capability as green, up to 30% loss as yellow, up to 50% as red, and anything beyond 50% as black. Of these values, I expected to see high variability in the measures of interest at the 15% level, with significant impacts at the 30% and higher levels. I again started with 10 iterations and spot-checked only a few combinations with 100 replications. None of the measures outputs varied by more than 10% from the baseline until
I crossed the 50% threshold, which the Army would consider a ‘red’ status. The results of the random deletions experiments are summarized below and then operationalized for both the strategic and operational models.

ORA™ executes the second immediate impact analysis using specifically named entity removal in what ORA™ terms impact analysis. In this method, the researcher specifies which nodes to remove from the model, and ORA™ again calculates and depicts the deltas between pre-removal and post removal network measures. This is what I refer to as targeted attacks in this section. Previous work (Kathleen M. Carley & Lanham, 2012) demonstrated nonlinear effects that cross a five percent (5%) threshold change in measures of interest with the top four entities in the Key Entity reports of the IT agents and IT resources. This dissertation revisited this effect by enumerating 1, 4, and 10 nodes for removal. These are clearly significantly fewer than 15% of nodes that I started with in the random targeting—reflective of the difference between random outages and adversaries’ efforts to deliberately create significant effects on friendly forces.

To decide which nodes to use in the targeted removal, it is necessary to make a short diversion into what the military calls defended asset lists and prioritized defended asset lists (PDAL). The next section enumerates an example of a PDAL for each model. I then draw from the PDAL for the targeted node deletions.

**Defended Asset Lists and Prioritized Defended Asset Lists**

Defended Asset Lists (DALs) and PDALs are, in their simplest incarnations, formal recognition of too few resources for too many demands. Each defensive asset (e.g., anti-aircraft artillery battery, network-based firewall) has finite reach and decreasing effectiveness against varying enemies at varying ranges. With this limitation—often called a limiting factor (LIMFAC) in the military, leaders make allocation decisions. Their task is to incorporate a mix of point defenses and area defenses—defending a few things well while balancing the desire to defend ‘everything’ from ‘everything.’ The Air Defense Artillery (ADA) community, theater missile defense, and strategic missile defense communities are examples of military planners and operations officers who expressly prioritize the importance of the assets they defend. These communities frequently use the CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability) method to provide a quantitative first round estimation that SMEs then refine and commanders approve. This dissertation’s modeling process can
contribute to such efforts by providing another quantitative basis to the decisions of what assets to prioritize based on their position in structural models.

Using this process, without consideration to political, public affairs, or coalition-maintenance considerations, extracts of the PDALs for the three models’ IT resources and IT systems might look like those below. Importantly, though the network analysis identifies key systems, SMEs for each system, the organization itself, and the providers, defenders, and maintainers of the communications methods can, and should, contact and expand the list to include necessary, but unmentioned, supporting technology(ies).

**Operational PDALs (IT System and IT resources)**

The operational model’s Key Entity reports lead to the contents of Table 47 below. ORA™ provides the seeds for the PDAL and organization SMEs refine the list to ensure the organization maintains the capability. The first such example is internet relay chat (IRC) capabilities—which ranked consistently higher than email. Presuming the IRC servers are not organic to the organization, paths to the servers and terminals to access the IRC servers become part of the capability on the PDAL in the second column, with comments or other pertinent information in the last column to maintain provenance for the entry.

<table>
<thead>
<tr>
<th>Primary IT System or IT Resource</th>
<th>Secondary or related IT System or IT Resource</th>
<th>Source / Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IRC Client (NIPR &amp; SIPR)</strong></td>
<td>x terminals (primary and backup) to access IRC server(s)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment between IRC terminals and servers</td>
<td>W/o network, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Primary and backup authentication</td>
<td>W/o login, IRC server unable to allow access</td>
</tr>
<tr>
<td></td>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote IRC server(s)</td>
</tr>
<tr>
<td></td>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
</tr>
<tr>
<td><strong>JOPES (Joint Operations Planning and Execution System)</strong></td>
<td>x JOPES terminals (primary and backup)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment between JOPES terminals and up/downlink(s)</td>
<td>W/o network, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
</tr>
<tr>
<td><strong>Traffic shaping device and rules</strong></td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
<td></td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>COP (Common Operating Picture)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x COP terminals (primary and backup)</td>
<td>Key Entity Report</td>
<td></td>
</tr>
<tr>
<td>VLANs and network equipment</td>
<td>W/o network, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>between JOPES terminals and up/downlink(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
<td></td>
</tr>
<tr>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
<td></td>
</tr>
<tr>
<td><strong>TBMCS (Theater Battle Management C2 System)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x TBMCS terminals (primary and backup)</td>
<td>Key Entity Report</td>
<td></td>
</tr>
<tr>
<td>VLANs and network equipment</td>
<td>W/o network, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>between TBMCS terminals and up/downlink(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
<td></td>
</tr>
<tr>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
<td></td>
</tr>
<tr>
<td><strong>GCCS (Global Command and Control System)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x GCCS terminals (primary and backup)</td>
<td>Key Entity Report</td>
<td></td>
</tr>
<tr>
<td>VLANs and network equipment</td>
<td>W/o network, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>between JOPES terminals and up/downlink(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
<td></td>
</tr>
<tr>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
<td></td>
</tr>
<tr>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
<td></td>
</tr>
<tr>
<td><strong>Telephone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x Landline telephone, encryption</td>
<td>Leader Directive</td>
<td></td>
</tr>
<tr>
<td>capable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure over to non landline</td>
<td>Continuity of Ops Planning</td>
<td></td>
</tr>
<tr>
<td>VoIP satisfactory iff traffic shaping device and rules prevent loss of service</td>
<td>Continuity of Ops Planning</td>
<td></td>
</tr>
<tr>
<td><strong>JWICS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>x terminals (primary and backup)</td>
<td>Key Entity</td>
<td></td>
</tr>
<tr>
<td>Strategic / permanent link</td>
<td>Terrestrial links usually have highest bandwidth</td>
<td></td>
</tr>
<tr>
<td>(terrestrial)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Uplink/Downlink capability</td>
<td>Backup (e.g., TROJAN SPIRIT like capabilities). Continuity of Ops Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Other entries as criticality, rehearsed backups/mitigations plans, resources, and other leader-specific criteria dictate
**Strategic PDALs (IT System and IT resources)**

The strategic model supports the same analysis though with a different set of capabilities present at the top of the PDAL. For this community the servers, data stores, authentication abilities, intervening firewalls between some defined number of terminals and the supporting servers become part of the package of ‘JOPES’ and ‘GCCS.’ Table 48 expands on the list of ORA™ listed capabilities, with the second column indicating necessary supporting abilities. The third column can provide rationale and continuity of knowledge between shifts and in the face of personnel turbulence.

<table>
<thead>
<tr>
<th>Primary IT System or IT Resource</th>
<th>Secondary or related IT System or IT Resource</th>
<th>Source / Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOPES (Joint Operations Planning and Execution System)</td>
<td>x JOPES terminals (primary and backup)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment between JOPES terminals and up/downlink(s)</td>
<td>W/o network, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
</tr>
<tr>
<td></td>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
</tr>
<tr>
<td>GCCS (Global Command and Control System)</td>
<td>x GCCS terminals (primary and backup)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment between JOPES terminals and up/downlink(s)</td>
<td>W/o network, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
</tr>
<tr>
<td></td>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
</tr>
<tr>
<td>COP (Common Operating Picture)</td>
<td>x COP terminals (primary and backup)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment between JOPES terminals and up/downlink(s)</td>
<td>W/o network, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Primary and backup authentication</td>
<td>W/o login, terminals are useless</td>
</tr>
<tr>
<td></td>
<td>Firewall rules</td>
<td>Avoid self-inflicted DOS by firewall to local and remote data stores</td>
</tr>
<tr>
<td></td>
<td>Traffic shaping device and rules</td>
<td>Preserve priority of traffic to local and remote data stores if necessary</td>
</tr>
<tr>
<td>GAMSS (Global Air Mobility Support System)</td>
<td>GAMMS terminals (primary and backup)</td>
<td>Key Entity Report</td>
</tr>
<tr>
<td></td>
<td>VLANs and network equipment</td>
<td>W/o network, terminals are useless</td>
</tr>
</tbody>
</table>
Targeted Assets

The next three tables (Table 49 to Table 50) list the nodes to remove during the targeted removal conditions of testing. The key entity reports provide these agents as a fast and justifiable listing of nodes that will be likely to inflict disruption on the owning organization(s). The deliberate targeting of capabilities on the PDAL and in the Key Entity report supports measuring the impacts of such removals—large impacts to the chosen measures of interest support the original forecasting.

### Table 49: Operational Model Nodes to Remove

<table>
<thead>
<tr>
<th>Total Nodes to Remove</th>
<th>Node Title</th>
<th>Node Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Relay Chat (IRC)</td>
<td>IT agents</td>
</tr>
<tr>
<td>4</td>
<td>IRC</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Joint Operations Planning and Execution System (JOPES)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Joint Warfighter Intelligence Communications System (JWICS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Defense Special Security Communications System (DSSCS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td>10</td>
<td>IRC</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>JOPES</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Common Operating Picture (COP)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Tactical Battle Management Command and Control System (TBMCS)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Global Command and Control System (GCCS)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Joint Warfighter Intelligence Communications System (JWICS)</td>
<td>IT Resource</td>
</tr>
</tbody>
</table>

Other entries as criticality, rehearsed backups/mitigations plans, resources, and other leader-specific criteria dictate
Results of entropic and targeted IT agents and IT Resource deletions

Overall, the entropic results confirm the previous work—random attacks against IT assets (systems or resources) have to rise to 30% or more of named assets to have effects on measures of interests that consistently cross a 10% change from baseline threshold. In the context of military battle damage assessment (BDA), for the twenty MoIs in use above, IT causalities have to rise to nearly a ‘red’ level for the effects of their total loss to move from ‘green’ to ‘amber.’ This broad result stands in stark contrast to the expansive statements of impending peril in the mass media.

However, broad results frequently have variability and nuance not well captured in sound bites or single sentence summaries. I will review the nuances of each of the measures of interest in the figures below. Each figure depicts in bar chart format the entropic deletion of nodes, replicated 20 times for each model. The heights of the bars are the percentage change from the baseline values discussed in the previous section. The color-coding matches previous color coding with blue representing the operational model and purple the strategic model. The height

<table>
<thead>
<tr>
<th>Total Nodes to Remove</th>
<th>Node Title</th>
<th>Node Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Joint Operations Planning and Execution System (JOPES)</td>
<td>IT agents</td>
</tr>
<tr>
<td>4</td>
<td>JOPES</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Common Operating Picture (COP)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Joint Warfighter Intelligence Communications System (JWICS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Defense Special Security Communications System (DSSCS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td>10</td>
<td>JOPES</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Common Operating Picture (COP)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Global Command and Control System (GCCS)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Army Data Distribution System (ADDS)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Global Air Mobility Support System (GAMSS)</td>
<td>IT agents</td>
</tr>
<tr>
<td></td>
<td>Joint Warfighter Intelligence Communications System (JWICS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Defense Special Security Communications System (DSSCS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Army Air Ground System (AAGS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Army Tactical Communications Systems</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Common Ground Station (CGS)</td>
<td>IT Resource</td>
</tr>
<tr>
<td></td>
<td>Directory services</td>
<td>IT Resource</td>
</tr>
</tbody>
</table>
of the like-colored lines represents the percentage change in the targeted node removals for each model. The X-axis has dual labels, with the integers representing the number of nodes removed and the percentage value representing the percentage of the IT agents and IT resource node set population removed.

The first MoI to check is the new measure of resilience.

The first two MoIs are the Characteristic Path Length and the Communication Speed of IT agents, Figure 107 and Figure 108 respectively. These MoIs are the inverse of each other so a discussion of both at the same time is appropriate. As none of the node removals involved the other node sets, there were no observed changes in this measure for any of the other networks in the model. As I expected, the targeted removal of small numbers of nodes in 600-1,000 node networks, did not in these models, nor is it likely in other models, have significant effects when aggregating at a network level. It is extremely interesting to note however that the removal of as few as ten (10) well-chosen nodes can have an effect as large as removing 50% of the IT agents.
and IT resources. As noted in numerous other studies, this effect is clearly the result of the
degree distributions of the underlying networks—power-law distributions are resilient to random
removals but highly susceptible to removal of hub nodes. With random outages (both self-
inflicted and others) being far more common than targeted outages, there is very little wonder so
many organizations perceive they can handle deliberate outages when they extrapolate from
random outages. A key take away from these two models, and the previous work of (Lanham,
Morgan, et al., 2011d), is that a few well chosen IT targets can generate the same effects as the
loss of 30% of IT resources for IT related MoIs.

Figure 107 Changes in Characteristic Path Length of IT agents for entropic and targeted deletions

Figure 108 Changes in Communication Speed of IT agents for entropic and targeted deletions
The next three MoIs paint very similar pictures in the effects at the IT system level. They all show the same pattern: targeted node removals yield results of similar magnitudes with an order of magnitude fewer removals than random attacks. The Density Clustering Coefficient in Figure 109, indicates that both models’ IT agents populations move further and further away from a small-world topology. The implication of this finding is that these IT systems will find it harder and harder to move messages between each other. This finding is not reflective of underlying technology protocols that support rerouting of information across operational links (e.g., EGRP or BGP in IP-based routers).

![Figure 109 Changes in Clustering Coefficient of IT agents for entropic and targeted deletions](image)

A related MoI is Diffusion. Diffusion typically requires a location node set inclusive of latitude and longitude (lat./long) information per location. When lat./long data is not present, ORA™ inference distances between agents by calculating and using geodesic distances instead—that is how far apart nodes are by hop count and link weight. In Figure 110, both models display a slightly nonlinear slow down in diffusion as the number of random and targeted nodes deletions goes up. Whether such diffusion slow down is significant for the organization is, of course, context dependent. The general finding should give pause to any leader tasked with working through and recovering from contested cyber environments.
The third of these related MoIs is Fragmentation and is shown in Figure 111. Here the pattern remains the same—increasing fragmentation as nodes get deleted. What stands out as prominent however is that the operational level organizations are more susceptible to IT system fragmentation than the strategic organizations. I had expected the reverse based on the professional observation that strategic IT systems are highly dependent on free-flowing information and they would be more vulnerable to system deletion and information disruption. One possible explanation could be that the strategic model had a high fragmentation score in the first place. It is reasonable to presume it’s hard to fragment an already fragmented network.
The next MoI, Isolate Count, behaved counter to expectations as seen in Figure 112, though a reasonable explanation is not difficult to find once faced with the modeled results. Intuition would suggest that the loss of IT agents and IT resources would lead to increased isolation of other, dependent systems. Results of random deletions however, as shown in Figure 112, lead to fewer isolates within the IT agents x IT agents network, not more. As noted earlier in this chapter, the IT agents node set, when examined in isolation, has 70 to 200 isolates for the tactical through strategic models. When examined within the entire metanetwork context however, the nodes are not isolates but connected to other node types. Given the high fragmentation rating for each model, it is no longer surprising that high quantities of random deletions would serve to reduce the over number of IT agent isolates. It is noteworthy that the targeted deletion of nodes had precisely the expected result, the increasing numbers of isolates!

Figure 112 Change in isolate count of IT agents for entropic and targeted deletions

None of the changes in Overall Complexity, Figure 113, rose above 4.5% change from baseline. These are large metanetworks with very low starting densities for each model. I had expected all deletions to lower the density, as with node deletion I expected link deletion. I had failed to incorporate the link distribution into my initial assessment and the results are visible in Figure 113. Random deletion is clearly deleting far more fragmented and low link count nodes, actually improving the over-all density, though the reader may recall the density improvement is insufficient to reduce the characteristic path length until 75% of the IT agent and IT resource nodes are deleted. The changes to the density with the targeted removal are in line with expectations both in the general trend and the magnitude of the decrease.
A more nuanced examination of density leads us a discussion of Social Density of IT agents—the network density of the IT agents x IT agents network in isolation from the metanetwork as a whole. In this MoI, Figure 114, we see that when focusing on the node set which is applicable to this MoI, there are, again, nonlinear results that differ dramatically by model. Random deletion is clearly not having much effect, with the high fragmentation values for each model. This type of variability and nuance is precisely what is lost in much of the opening paragraphs of related cybersecurity literature. IT specific effects may be significantly different than results aggregated across multiple viewpoints.
The last MoI of this chapter is by far the most interesting and one with interesting variability. Performance as Accuracy is a measure I applied to three node sets in each model: agents, IT agents, and roles. In that order, I’ll discuss the findings of the static targeted and entropic node removal impact analysis. When considering just the human agents as problem solvers, there were essentially no effects in the targeted and entropic deletion efforts—no model nor deletion condition led to changes larger than 6% from baseline! As seen in Figure 115, the strategic model had improvements as we deleted random IT agents and IT resources, as did the tactical model and the operational model with one exception. This result may not generalize to all organizations with perceptions of IT dependence—it certainly is counter to numerous public assertions that the American military could be paralyzed by a cyber attack. Even the targeted deletions have very little effect, and not consistently negative either. This too was counter to expectations, but reinforcing earlier work! Though worthy of exploration in live exercises and events, it is possible that far more task knowledge and situation knowledge exists with people in these organizations than the cyberthreat-focused analysts give credit for.

![Figure 115 Changes in Performance as Accuracy of Agents](image)
When using the rapid model construction process of this dissertation, and the D2M model in general, one of the output node sets is ‘Roles.’ This node set consists of generalized positions filled by more than one person, so broadly discussed it does not easily map to a single person. These kinds of entities are frequently in doctrine documents or other organizationally generated documents. As such, it is appropriate to examine the impact of removing access to IT agents and IT resources on these types of organizational members. As shown in Figure 116, the impacts are mixed and do not present a clear picture. The impacts are consistently low (all below 1% change from baseline) and as such it is unwise to overly generalize the results both within the two modeled organization types as well into organizational resilience to contested cyber environments.

When disaggregating IT agents from other agents, Figure 117, the impacts of entropic deletions correspond almost exactly with the color coding scheme of the Army: 15% loss of systems equates to approximately 15% loss of accuracy and the consequent color-coding change from Green to amber/yellow. Likewise a 50% loss of random systems equates to a 50% drop in accuracy, moving from yellow to red, and bordering on black. Across these three models, and one other model from previous work, there is now an established trend that random loss of
availability of IT systems and IT resources may not have overt large-scale effects unless the loss crosses a leadership-defined threshold.

Importantly though, the same trend exists for targeted losses, to which organizational leaders must pay very close attention. Loss of Key-Entity-identified-systems, when combined with each other, rapidly causes nonlinear results in very small quantities! In these models, the loss of four capabilities (two (2) IT agents and two (2) IT resources, without expressly considering the mechanisms for their loss) causes the same drop in this MoI as the loss of 15% of the original node populations (see also node populations in Table 19). In these models, deletion of as few as ten (10) nodes, when carefully selected, can create effects as large as a random loss of 50% of the nodes.

![Figure 117 Changes to performance as accuracy of IT agents](image)

**Conclusion**

The dissertation as made the case that over time resilience assessments are fundamental to assessing mission assurance to contested cyber environments. To conduct assessments, leaders and analysts must start with one or more baselines—this chapter is the baseline for comparison of future time points. This chapter has demonstrated the application of existing social network analysis and metanetwork analysis measures against two doctrine generated models. The chapter
has also introduced and demonstrated the calculation of a new metric, that takes into account the specialization of organizational functions and components. This measure is a weighted function of the near isolation of tasks, resources, and knowledge, over-supply of knowledge and resources to organizational tasks as well as shortfalls of the same. The new measure assists decision makers through adding an additional dimension of resilience through redundancy of capabilities as well as redundancy of access to capabilities—it does not provide a single ‘magic number’ that can signal “All is well” or “Brace for Impact.”

The most important take away from this chapter is that the rapid modeling process of the previous chapter can generate an model subject to analytic efforts that demonstrates a recognizable, though nonunique, outcome: targeted removal of IT systems and IT resources in complex sociotechnical organizations can lead to effects disproportionate to the number of directly affected systems and resources. This trend leads to a lesson for organizational leaders that the risk management community has incorporated for a very long time: identify the most important systems and resources and ensure their continuity of operations at some \textit{a priori} acceptable level. The decision process that identifies those important functions and capabilities can use the techniques in this dissertation as a mechanism, as well as supporting or supplemental means—the key is the realization that a few well-chosen losses will predictably have outsized impacts! This phenomenon has earned the moniker ‘black swan event’ in some circles though it is by no means the only descriptor.

In the next chapter, I move from the static, point-in-time assessments to a forecasting methodology using D2M derived models and agent based cognitive simulations. Forecasting how organizations adapt to a contested cyber environments can be a useful tool for leaders to use in what-if scenarios and general-purpose cyber resilience discussions.
“All models are wrong, but some are useful.” (Box, 1979)

Agent Based Models and Modeling

This chapter of the dissertation will review related agent based model (ABM) work in sociotechnical systems and cyber security research. I will also provide a brief discussion of how the CASOS ABM capability called Construct (Frantz & Carley, 2007; B. Hirshman et al., 2011) operates. These set the stage for a detailed discussion of model preparation and experimental design that I use to demonstrate the resiliency score over time as well as the other indicators of resilience performance.

In brief, the experimental scenario applied to two (2) empirically based models derived from the models discussed in the previous two chapters. In addition to baseline conditions (no attacks of any variety), the experiments involved creating and assessing the effects of cyber attacks in the form of integrity and availability attacks aimed at specific systems, a generalized confidentiality attack, and availability attacks aimed at communications infrastructure between agents. I expected, and simulation experimentation confirmed, varying effects on selected network measures discussed in the last chapter. Importantly, the scenario then added four possible mitigations to the simulation to assess their efficacy—and demonstrating in simulation that networked organizations can adapt to misfortune and assure leadership of their resilience.

The operational scenario for each model was based on the first few steps of the military decision making process (MDMP): receive a plan and conduct a cycle of mission analysis/planning and briefing of leadership. These steps are, under different names, nearly identical in all organizations tasked with receiving direction from others, planning how to implement those directions, communicating the plan to subordinates, and executing the plan. I represented the OPORD by adding, exogenously, a set of ‘plan’ bits to the set of knowledge bits the D2M process had discerned. I assigned these ‘plan’ bits to the key IT Agents identified using key entity reports. The agents linked to the agent group named “joint planning group” had the task to plan amongst each other (e.g., interact with each and exchange information) then brief organization leadership 3 times during the first one-third of the simulation time. I also added a set of ‘bad plan’ bits for use by the attacking integrity agent. Using a Box-Behnken Response Surface Modeling design, I varied the probability of effects of each of the six attacks vectors, as well as four mitigation efforts, for a total of ten quantitative variables.
The cyber losses, when enabled, occur during the midst of the plan-brief-plan-brief cycle. I expected, and the simulations experimentation confirmed effects dependent on the probability of effect, the mitigation in place (if any), and the speed with which the mitigation is put in place.

**ABMs and sociotechnical systems**

ABMs are ideally suited for developing theories of and exploring via simulations, situations where the modeled entities, as individuals, must perceive and react to their modeled environment(s). When those situations are not conducive to human-subjects studies, simulations using agents help bridge gaps between theory in isolation, theory based on extrapolation from human-subjects studies, and being unable to pursue resolutions to research questions of interest.

ABMs are not the only method of modeling for these situations, as previously discussed in the related literature portion of the dissertation. When the question at hand is continuous flow or process related across well-defined paths, dynamic systems may be a more appropriate vehicle for developing theories of flow (Borshchev & Filippov, 2004). When questions at hand have no interest in forecasting the effects of multiple individuals’ actions in an artificial landscape, abstracting the individuals away into sets of equations, sources, sinks, and interference patterns may be a better approach for a researcher. When a researcher wants to study aggregations of entities (e.g., organizations) free from cognitive limitations, there is unmistakably no need to complicate their abstraction with per-entity limitations, or even low-level entities at all! Of course, ABM offers exactly the opportunity for low-level decisions, behaviors, and observables to, without a priori rule writing, discover explanatory mechanisms for what appear as deliberate or purposeful crowd-level phenomena. Indeed, a key aspect of a properly designed and built ABM experiment is to ensure that whatever constraints and impulses do exist in the model, they are not artificially driving the result to an aggregate-level outcome through over-controlling the agents (J. H. Miller & Page, 2007).

Examples of ABM use applied to questions of aggregated-level phenomena include theorizing about which organizational designs cope better with communication breakdowns at agent levels (Kathleen M. Carley, 1991; DHS, 2011). OrgAhead is another example of ABM used to improve patient care at the unit-level (Effken et al., 2005), evaluate team performance in the face of turnover when interactions include face-to-face as well as technology-enabled mechanisms (Levine, Moreland, Argote, & Carley, 2005). Indeed Levine’s work, using a code-
base predecessor of Construct, validated the results of the ability to generate realistic patterns of behavior among artificial agents as well as generated aggregated results congruent with human-subject experiments. Canessa’s work using ABM was another effort at demonstrating replication of emergent behavior from collections of agents interacting with and without the aid of technology (Canessa & Riolo, 2003). That work also demonstrated structure/network-based effects mediated by technology as well as the effects of out-of-group forced interactions on intra-group performance. The breadth of examples of researchers using ABM to help build and test theories is well beyond the scope of this dissertation to cover. What is notable however are the research areas between these examples of ABM applied to sociotechnical systems and current incarnations of cybersecurity research and the desire to protect continued use and access to the technical components of those systems. Those research areas remain ripe for study, as demonstrated in the paucity of cross-domain collaboration of authors in their respective areas of expertise and discussed in the Literature Review chapter and specifically in the Related Areas of Research section.

**ABMs and cyber security research**

Cyber-security research, especially when constrained to technology-focused models and questions of interest have ventured into the ABM realm less frequently than many other fields of research. This is certainly understandable when viewing computer network traffic as continuous flows of data packets, where individual packets, and even individual components of the network have little to no ability to perceive their environment and react to it. It is this broad view that is a common theme in the network emulators in (Lochin et al., 2012) review. Even in the pursuit of ‘intelligent’ networks and machine adaptation to network or component level challenges (e.g., component outage, rate control services (Gligor, 2005), load-balancing redirection (Pai et al., 1998; Wang et al., 2002)), the agents are not human agents, nor are the researchers usually making the leap to incorporate the sociological component of sociotechnical systems in the section title. In one NSA-sponsored cybersecurity forum, the organizers even went so far as to constrain discussions by omitting ‘humans’ because ‘they are hard to understand’ and it’s much less contentious to work on the technology side of research questions.

There have absolutely been efforts at evaluating the human-impacts of disruptions to or loss of the technical infrastructure. The research gap remains however between those efforts and
the continuity of operations COI, the HRO COI and other efforts to understand the world we live in, especially when the world changes quickly or dramatically. Some efforts have incorporated human-enabled process modification (e.g., employing off-line backup capacity) (Pflanz, 2012; Pflanz & Levis, 2012) as a way of assessing the sustainability of time-sensitive missions in cyber-degraded environments. Others, such as RINSE (Leblanc et al., 2011) support Live and Constructive integration of human role players and simulations of technology as does the Department of Defense’s Bulwark Defender exercise (Wihl et al., 2010). Multimodel modeling is also an approach to Incorporating ABM M&S with technology focused M&S (Bigrigg et al., 2009; Kathleen M. Carley, Geoffrey P. Morgan, et al., 2012; Kathleen M. Carley et al., 2012; Elder & Levis, 2010). The cited examples have demonstrated modeling working in tandem though not interoperating. The methods would seem to offer fertile opportunities for researchers to use models with varying processing and generative internals. When outputs are congruent, researchers can reasonably argue higher confidence in the feasibility of the results.

This section has been a short refresher of the material discussed in Literature Review chapter. The intent has been to remind the reader that there are many related fields of research that a casual observer could reasonably infer share interests and information. The potential for such sharing of theories, methods, results, and understanding certainly exists, and this dissertation is but one example of a way to link related-yet-disparate research: technology enabled and dependent organizations’ resilience to contested cyber environments.

Overview of Construct

Construct is an ABM developed over time at Carnegie Mellon University under the guidance and supervision of Dr. Carley. It has its roots in constructualism (Kathleen M. Carley, 1986), the view that the inhabitants of socio-cultural environments continually construct and reconstruct their environment through individual cycles of action, adaptation, and motivation. It is network-centric not only in its roots but in its implementation, internal data structures are frequently matrix representations of those networks—a sight familiar to practitioners of social network and graph-theoretic sciences. Construct has had numerous technical reports written since its inception, and I refer the reader to its User’s Guide (Kathleen M. Carley et al., 2014), predecessor Technical Reports and CASOS for up-to-date information and changes from its
documentation. This section will provide a brief overview of Construct’s origins and internal functioning.

Initial instances of Construct had basic interaction mechanisms that embodied three (3) empirically identified human interaction generalizations. The first is that knowledge acquisition occurs through interaction (Leon Festinger, 1950) as cited by (Schreiber, Singh, & Carley, 2004). The second is that humans tend to interact with those who are similar to them, often called homophily and described in (J. M. McPherson & Smith-Lovin, 1987) and revisited by those authors in (M. McPherson, Lovin, & Cook, 2001) among many others. The third interaction pattern is social relativity, first discussed by Festinger (1954) and (Merton, 1957, 1968) (as cited by (Schreiber et al., 2004)). These three (3) patterns had up to five (5) moderators available to a researcher to use in experiments: forgetting, proximity, transactive memory, referrals, and access (Schreiber et al., 2004).

The roots of Construct as an information diffusion simulation are evident in the first interaction pattern and the principal motivation of agents in the simulation—the drive to interact with other agents to exchange information. The moderators of that drive are the agents’ perceptions of similarity to other agents (transactive memory (Argote, 2003; Ren & Argote, 2001) and homophily) as well as proximity and synchronous availability. Knowledge retained and propagated has, as moderators, the forgetting rate(s), as well as stochastic probabilities of mishearing a message from other agent(s) as well as misstating knowledge when sending it.

Subsequent and modern versions of Construct added binary task completion and energy tasks (Moon, 2008) to the simulation. Binary tasks are used in traditional methods of studying organizational accuracy. Participants in the task attempt to discern the number of ones (1) or zeros (0) in a binary string, and pass their estimations or answers to others. Knowledge bits, pools of binary values representing knowledge available to agents, have links to these tasks (in the form of a Task x Knowledge network). These networks support the intuitive property that possessing higher quantities of linked knowledge leads to higher probabilities of agents and groups of agents accurately performing these tasks. In the absence of knowledge, agents must still make assessments and do so using reported assessments of agents to whom they are connected. Energy tasks are abstracted nonspecific tasks that reflect the reality of human agents.
not spending their entire existence only talking with other agents. When enabled, agents will spend some portion of their simulation

Belief diffusion, an extension of knowledge diffusion and tied to the social relativity work of Festinger and others is in current-day versions of Construct. Real numbers ranging \([-1, 1]\) represent each stylized belief per agent. In this range of values, -1 represents a maximal negative valence and 1 represents a maximal positive valence to the belief. Researchers may create modeled beliefs rooted in possession of knowledge that contributes to positive or negative valence as well as modeling beliefs not directly related to knowledge. Self-perception as well as omnipotent knowledge of other agents’ beliefs contribute to homophily assessments and increase the probability of interactions—at the expense of increased computational time.

The final aspect of Construct to briefly discuss is its recent incorporation of social groups and generalized other (Mead, 1925) as cited in (Joseph, Morgan, Martin, & Carley, 2013). Joseph et al. adjusted Construct away from agents retaining perceptions of every alter-ego to which the agent has connection. In its newest incarnation, Construct agents, when faced with having no personalized perception of an alter, and consequently no basis to judge homophily, create an error prone interpretation of the alter based on knowledge of the social groups the alter belongs to (Joseph et al., 2013). This social stereotyping is akin to not personally knowing a political candidate, but inferring the candidate has certain beliefs and knowledge based on the avowed political party of the candidate. If there is no information about the group(s) the person belongs to, then inferences occur based on a people-in-general concept, often referred to as the generalized-other (Mead, 1925).

Through creation of appropriate input files, what the Construct’s User Guide (Kathleen M. Carley et al., 2014) calls input decks, researchers provide Construct definitions of experimental variables, lists of input nodes, and network definitions. Construct can stochastically generate the networks using parameters in the input deck, read data from ORA™ DynetML files, or draw from other empirical sources. Node identifiers can also be from empirical sources, or simple integers from \([0..n]\) with \(n=number\ of\ nodes\). I refer the reader to the Construct User’s Guide for a more complete discussion of the input deck contents and to Appendix 5 for the deck I used for the operational and strategic modeling.
Augmentation of D2M generated and stylized models

There are two models of organizations (organization being an aggregation of multiple heterogeneous cognitively limited agents) I use in the dissertation: strategic and operational. To use the D2M and stylized models created in previous chapters, each requires a level of augmentation. Revisiting the dissertation workflow from Figure 36, we can see where we are in the process by looking at the colored ovals and box in Figure 118.

The source documents I used do not discuss many of the particular inputs Construct needs to function, though this shortfall is likely more manageable with use of proprietary or sensitive documents instead of public documents. Additionally, the initial modeling effort deliberately used the entire ontology for metanetwork node types. Not all the node types in the metanetwork ontology are useful to Construct which leads to both descoping the metanetwork model as well as augmenting it for processing by Construct.

The table below is roster of changes and modifications to the metanetwork ontology. There are a total of thirty modifications needed on the D2M model for Construct to be able to make complete use of the model.

![Diagram of dissertation workflow augmentation of models for use in ABM]
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
</table>
| 1.    | Added    | agent node set   | Where I had no data to discern a classification level, I created a new instance of the agent or IT agent. I assigned this new instance the ‘level 2’ attribute and assigned ‘level 1’ to the D2M-identified agent or IT agent.  
In this manner, a geospatial_database IT agent would get a twin called  
geospatial_database_level2.                                                                 |
| 2.    | Added    | agent node set   | I manually create a confidentiality sink agent and assigned it a ‘level1’ attribute for each model.  
This agent is responsible, when active during confidentiality attacks, for receiving communications from other IT agents. Assessment of the organization is the tendency of  
level2 knowledge to flow to and within level1 agents—representing a classification leak though without specific operational impacts.  
Assignment of links to level1 key IT agents used the same random binary graph generator and equation (40) |
| 3.    | Added    | agent node set   | I manually create an integrity agent for each level of each model.  
This agent is responsible, when active during integrity attacks, for disseminating bad information into the organization.                                                                                             |
| 4.    | Added    | agent node set   | Roles do not exist in Construct. I recoded all roles as agents, though I retained an attribute on the imported roles listing them as ‘role’                                                                 |
| 5.    | Added    | agent node set   | I recoded all IT agents that the D2M process generated as construct agents. I did however retain an attribute that labels the recoded agents as ‘it_systems.’  
Construct supports different behaviors for different agent types, and the IT agents have a reduced probability of forgetting, higher quantities of communication reception counts than human agents. IT Agents have the same communications initiation counts as human agents, and with the disparity between initiate and receive, they are more akin to ‘pull’ IT systems than ‘push’ IT systems. |
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Added nodes</td>
<td>knowledge node set</td>
<td>Where I had no data to discern a classification level, I created a new instance of the knowledge node. I assigned this new instance the ‘level 2’ attribute and assigned ‘level 1’ to the D2M-identified knowledge node. This heuristic possibly over generalizes the amount of information in an organization but it decreases processing time for model generation. It also acknowledges that a knowledge concept may well reside with two (2) slightly different instantiations: unclassified and classified.</td>
</tr>
<tr>
<td>7.</td>
<td>Added nodes</td>
<td>knowledge node set</td>
<td>I manually created a set of knowledge equal to 10% of the knowledge set to represent a ‘plan.’ 10% of plan knowledge received a ‘level 1’ attribute 90% of plan knowledge received a ‘level 2’ attribute</td>
</tr>
<tr>
<td>8.</td>
<td>Added nodes</td>
<td>knowledge node set</td>
<td>Manually created ‘bad plan’ knowledge at ratio of 10:1 (good:bad) for level 1 and level 2. Manually assigned these two sets of knowledge to their respective knowledgegroup. Manually assigned integrity agent level 1 to bad plan knowledge level 1. Manually assigned integrity agent level 2 to bad plan knowledge level 2.</td>
</tr>
<tr>
<td>9.</td>
<td>Added nodes</td>
<td>knowledgegroup node set</td>
<td>I manually segregated the D2M generated knowledge pool into five (5) major groups, and eleven total sub-groups. The dissertation is asking questions about the resilience of planning organizations in the face of contested cyber environments. But having only ‘information of interest’ in the simulation is a degenerate design case and uninteresting from a research perspective. 1. All_knowledge 2. General_knowledge 2.1. General_knowledge_level1 (all level 1 non-plan knowledge) 2.2. General_knowledge_level2 (all level 2 non-plan knowledge) 3. Plan_k 3.1. Plan_knowledge_level1 (see next row for details) 3.2. Plan_knowledge_level2 (see next row for details) 4. Bad_Plan_K 4.1. Bad_plan_knowledge_level1 4.2. Bad_plan_knowledge_level2 5. No Bad K (General_K + Plan_K)</td>
</tr>
<tr>
<td>Item #</td>
<td>Action</td>
<td>Of What</td>
<td>Why and Discussion</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>---------</td>
<td>--------------------</td>
</tr>
<tr>
<td>10.</td>
<td>Added nodes</td>
<td>Location node set</td>
<td>I added nodes for the headquarters of all the commands of interest. For those commands where I did not have an exact location I used Google Maps and a general search to provide a latitude and longitude (e.g., Al Udeid Air Force Base, Doha, Qatar) I also added an ‘other’ node for those organizations for which I had no evidence of an actual location. This was particularly true for IT systems. For the geographical location of this other, I chose Fort Knox, Kentucky as it was somewhat near the geographical center between Washington DC and Barksdale AFB for the Strategic Model. For simplicity I left it the same for the Operational model as well.</td>
</tr>
<tr>
<td>Item #</td>
<td>Action</td>
<td>Of What</td>
<td>Why and Discussion</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>11.</td>
<td>Added nodes</td>
<td>organization node set (aka agentgroup)</td>
<td>I added a JPG group and ‘JPG Briefing’ groups to each model’s organization nodeset.                                                                                                 The dissertation is asking questions about the resilience of planning organizations in the face of contested cyber environments. Focusing on the planning nature of these organizations, allows me to have a set of agents (the JPG) that receives a ‘plan’ from some exogenous source. A method of assessing organizational resilience is to trace the flow of plan information from this JPG to the remainder of the agent population. More specifically, the dissertation attempts to identify differences in uncontested environments and contested environments in the speed and accuracy of information flow to the various sets of decision makers (the attendees of the JPG Briefings) in the models.</td>
</tr>
<tr>
<td>12.</td>
<td>Deleted nodes</td>
<td>Belief node set</td>
<td>Incorporation of beliefs was beyond the scope of this effort. I deleted the entire belief node set.                                                                                                                     Future work could easily generate questions of interest and incorporate beliefs into future models.</td>
</tr>
<tr>
<td>13.</td>
<td>Deleted nodes</td>
<td>Event node set</td>
<td>The only specific event modeled in the scenarios under test was the plan-brief-plan cycle.                                                                                                                             Construct could not draw this cycle from the list of events the D2M process generated, so Construct does not use these nodes or networks.</td>
</tr>
<tr>
<td>14.</td>
<td>Deleted nodes</td>
<td>IT Resources (aka Communications Mediums)</td>
<td>I deleted all the IT resource nodes in the D2M generated models and kept seven (7) nodes per model. These nodes are what Construct calls ‘Communications Mediums.’                                                                                                                     For any two agents to interact, not only must they have a connection in the agent x agent network, they must both have access to a common communication medium.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unclassified Telephone/Voice</td>
<td>1. Unclassified Telephone/Voice</td>
</tr>
<tr>
<td>2. Classified Telephone/Voice</td>
<td>2. Classified Telephone/Voice</td>
</tr>
<tr>
<td>5. Face-to-Face (f2f)</td>
<td>5. Face-to-Face (f2f)</td>
</tr>
<tr>
<td>6. Unclassified Email</td>
<td>6. Unclassified Email</td>
</tr>
<tr>
<td>7. Classified Email</td>
<td>7. Classified Email</td>
</tr>
</tbody>
</table>

172
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>Deleted</td>
<td>organization node set (aka agentgroup)</td>
<td>I down selected organizations, manually, in the D2M models to a set of suborganizations of interest as noted below for each of the two models. I manually deleted organizations with less than 3 x D2M-discerned edges in them—with the exception of the manually added groups (e.g., confidentiality agent group, and integrity agent group) and groups necessary to maintain organizational face validity. I added groups for assessing collections of agents that the D2M process did not otherwise capture. See also the entry for adding nodes to the organization node set.</td>
</tr>
<tr>
<td>16.</td>
<td>Deleted</td>
<td>Location node set</td>
<td>I deleted all nodes that did not have a geographically identifiable location (e.g., Barksdale Air Force Base).</td>
</tr>
<tr>
<td>17.</td>
<td>Deleted</td>
<td>Resource node set</td>
<td>Resources do not exist in Construct with its origins in belief and information diffusion. I deleted the entire resource node set the D2M process generated.</td>
</tr>
<tr>
<td>18.</td>
<td>Added</td>
<td>agent nodeset</td>
<td>The corpus rarely discussions clearance requirements for roles and individuals. For each human and IT agent, I assigned them a node attribute of ‘human’ or ‘it_system.’ The corpus rarely identified IT systems as ‘IT systems’ and usually simply referred to generic IT systems or named and specific systems. I therefore manually reviewed each of the retained agents to identify if they were ‘human’ or ‘IT.’</td>
</tr>
<tr>
<td>Item #</td>
<td>Action</td>
<td>Of What</td>
<td>Why and Discussion</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 19.    | Added node attributes | knowledge nodeset | Differentiation of sensitive and nonsensitive knowledge The D2M corpus rarely directly differentiates which knowledge concepts belong to which levels of classification domains. To remediate this shortfall, and assist in the rapid modeling process I used the following heuristics and methods to segregate the single knowledge node set into two nodesets.  
- Knowledge nodes connected only to IT systems (Level 1) stayed in level 1 knowledge  
- Knowledge nodes connected only to IT systems (Level 2) stayed in level 2 knowledge  
- Logistics, Medical, and Personnel ‘intel,’ and ‘plan’ nodes stayed with level 1, while military operations centric intel nodes stayed with level 2  
- All publications stayed with level 1 knowledge |
| 20.    | Added edges | agent x agent network agent x organization network organization x organization network | Most organizational models, to at least establish face validity, need to reflect lines of authority. The D2M process did not always capture the chains of command a reader would expect of military organizations. The D2M corpus frequently did not adequately reflect the details of the command hierarchies for both levels of warfare.  
As such, a manual process of edge creation in the agent x agent, organization x organization, and agent x organization networks based on SME input and my own professional expertise was necessary to augment the automation-based models with additional relationship edges between organization nodes. |
<p>| 21.    | Added edges | agent x agent | When I duplicated agent nodes to create ‘level2’ agents, I needed to duplicate the edges each ‘level 1’ twin had, but inside the ‘level2’ agent set.  (39) |</p>
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
</table>
| 22.   | Added edges   | agent x agent                    | When I created integrity agents, I needed to have them connect to other agents to enable dissemination of their information. I chose to target the Key IT systems as the targeted systems, based on the static assessments of large effects created by targeting small but important quantities of IT systems.  

I used a random binary graph generator within Construct with a mean value set with the equation shown below. In other words, if the probability of an integrity attack was 0.8, the integrity agent would have a probability of 0.8 for receiving an artificially created link between it and any particular key IT agent.  

\[ P_{\text{interaction}} = \begin{cases} 1, & \text{random}<\text{Probability}_{\text{integrity attack}} \\ 0, & \text{else} \end{cases} \]  

(40)                                                                                                                                 |
| 23.   | Added edges   | Agent x communications medium network | I manually created links between agents and communications media using the following heuristics:  

- Human (level 1 and level 2) to human (level 1 and level 2): f2f, level1 phone  
- Level 2 Human to Level 2 Human: level 2 phone, level 2 email  
- Level 1 Human to Level 1 IT Agent: level 1 IP network  
- Level 2 Human to Level 1 IT Agent: level 1 IP network  
- Level 2 Human to Level 2 IT Agent: level 2 IP network  
- Level 1 IT Agent to Level 1 IT Agent: level 1 IP network  
- Level 2 IT Agent to Level 2 IT Agent: level 2 IP network |
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.</td>
<td>Added</td>
<td>edges</td>
<td>Organizations (aggregations of humans for common purposes/tasks) do not exist as explicitly modeled entities in Construct. Instead, modelers can exogenously assign agents to groupings of Agents that help fulfill the stereotyping of perceived similarity capability. Such grouping also supports output analysis at various levels of aggregation. The Agent x Organization links derived from the D2M process are far too sparse to support the Construct group membership stereotyping. I added edges between agents and organizations that I knew existed based on my military experiences. I also added edges based on samplings of the corpus.</td>
</tr>
</tbody>
</table>

Figure 120 Agent x Communications Medium (Operational)
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
</table>
| 25.   | Added edges          | agent x organization organization x organization | After I manually created the JPG and JPG Briefing Group for each model I created links between elements habitually included in JPGs (e.g., intel, ops, ops planners, logistics planners, staff judge advocate, targeters).
|       |                      |                                              | The D2M models may have words that semantically mean JPG briefing, but there is no other sense of a time-driven event in the D2M models. Instead the plan-brief-plan cycle is implemented using the following heuristics within the simulation:
|       |                      |                                              | - 1/3 of the time period after the simulation warm-up is set aside for ‘planning.’
|       |                      |                                              | This corresponds to a military heuristic of 1/3:2/3 time division between the planning organization and the implementing organization.
|       |                      |                                              | - A starting value of 20% of the ‘planning’ time is set aside for ‘briefings’
|       |                      |                                              | - The JPG is incentivized to interact with each other by more heavily weighting expertise seeking behavior during the plan-brief-plan cycle.
|       |                      |                                              | - There is a large group of
| 26.   | Added edges          | Organization x location                      | I manually created links between the organizations of interest and the locations of interest.                                                                                                                                                              |
| 27.   | Deleted edges        | Agent x knowledge network                    | I manually removed links between level 1 Human and IT agents and level 2 knowledge. I allowed level 2 agents and systems to remain connected to level 1 knowledge.                                                                                                    |
| 28.   | Edge modification    | agent x agent network                        | I binarized the agent x agent interaction network the D2M process generated. Edge weights were co-occurrence counts in the source documents, and otherwise not of benefit to the simulation process.
|       |                      |                                              | Co-occurrence counts for the IT systems, especially after sampling and reading source documents indicate a common interpretation: there is some logical inter-dependency of the systems. An example of this would be a web server linked to a database is representing a logical dependency with the actual physical or network-level interconnection abstracted away from the model. |
| 29.   | Warm Up Period       |                                              | As noted in Figure 2 and Figure 85, I use a warm up period to establish an equilibrium point in the organization prior to executing attacks.                                                                                                               |
| 30.   | Added network        | Physical proximity network                   | Construct supports inferring a distance measure thorough the use of geodesic distances and edge weights, but I felt decided to use geographical distances, scaled and inverted as                                                                 |

177
<table>
<thead>
<tr>
<th>Item #</th>
<th>Action</th>
<th>Of What</th>
<th>Why and Discussion</th>
</tr>
</thead>
<tbody>
<tr>
<td>31.</td>
<td>No Change</td>
<td>Task node set</td>
<td>I did not differentiate sensitive and non-sensitive tasks. The implication is that such tasks can require level 1 and level 2 personnel and knowledge.</td>
</tr>
</tbody>
</table>

Construct expects—a distance of 1.0 indicates two agents are maximally close, while a distance of 0.0 indicates the agents are maximally distant.
Adversary definition and setup for contested cyber environments

Instead of developing an adversary with a defined set of capabilities and motivations, this dissertation moves directly to predicted and simulated effects of an adversary’s actions. In this effort, adversaries have, implicitly, finite capabilities and implicit motivations. The scenarios put under test here demonstrate an approach well beyond negligible threat, but equally well short of omniscient threat. I do make overt assumptions about adversarial capabilities, but in a direction orthogonal to the warnings of adversarial assumptions and resulting bad policy (Gligor, 2008).

Each of the three effects under test in the next chapter, loss of confidentiality, loss of integrity, and loss of availability are mid-term effects of a cyber attack. The loss, from near zero to total, of any of these three pillars of information assurance and security, are in themselves, rarely the sought-after effect in contested cyber environments. Rather, they are a component in efforts to deny friendly forces synchronized command and control of resources, with the subsequent effect of creating opportunities (e.g., military advantage, commercial advantage, possession of intellectual property, embarrassment, criminal opportunities) for an adversary to exploit. By inserting attack agents into each model at each classification level to act as a source for ‘bad’ knowledge to diffuse within the organization, I am implicitly granting my nameless adversaries the capability to conduct actions akin to advanced persistent threats (APT). The adversary has at his/her disposal, in each of the integrity attack conditions, the ability to inject bad data into the friendly organizations. Previous work (Lanham, Morgan, & Carley, 2012) has already demonstrated that with no screening criteria for clearly ‘bad’ knowledge, an adversary can have bad information diffuse throughout an organization. The same work also demonstrated that the bad knowledge, even if given an extremely short time-to-live, is incredibly long-lived: in general up to an order of magnitude longer than the original injection time!

In the loss of availability scenarios, I again choose to not posit a particular scenario that lead to the loss of key IT system availability—I simply assert there are instantaneous losses of availability at specified times. I grant the adversary (e.g., a malicious person, persons, nation-state, natural weather event) the ability to temporarily render one or more agents inaccessible while making the motivations of the contested cyber environment opaque. In this way, I’m attempting to avoid the numerous arguments and point/counter-point debates about plausibility and instead move to the more important aspect, for this dissertation, of assessing post event
resilience. I do not dispute the arguments by Cohen (F. Cohen, 1999) and Leblanc (F. Cohen, 1999; Leblanc et al., 2011) that adversary models should include capabilities and resource. Nor do I dispute that when research questions involve adversary motivations that scenarios and experiments should address such as advocated by (Gligor, 2008; Parker et al., 2004). The absence of these pieces of adversarial information is indicative that the information is not essential to the study of resilience to posited adversary-caused effects.

Finally, for the loss of confidentiality effect, I have chosen to model an adversary who is not pursuing an aggressive penetration and exploitation style of cyber attack. The technique I have chosen is to mimic a passive device targeted at ‘key IT systems’ and whose purpose is to collect data. It is an imperfect data capturing device, and is active at only specified time periods. This is a very general form of a confidentiality threat, much less than a key logger, and yet more than a data sniffer on a random piece of hardware. I do not attempt to assert a particular motivation for the confidentiality agent, nor do I have a particular end state for what some remote adversary would do with the captured data.

**IT capabilities for D2M and stylized organizational models**

Underlying telecommunications and networking infrastructure systems (e.g., TELCO POPs, signal regeneration points) are abstractions contained but not otherwise addressed in the Construct simulation’s implementation of communications mediums. As noted in Table 51, both D2M generated models have communications mediums of face-to-face, email, phone, and IP-based networks (the only way for IT agents to interact with other agents of any variety). Each of these mediums exist at each of the security levels. This gives a total of seven (7) communications mediums per model.

**Classification levels for D2M and stylized organizational models**

Organizations, civilian and military, frequently handle information and communications at several levels of sensitivity. In the military, these are typically the classification levels of unclassified (with and without handling caveats such as *For Official Use Only*), secret (with and without compartmentalization indicators), and top secret (with and without compartmentalization indicators). Civilian organizations may or may not use these same levels, but this proposal makes the simplifying assumption that both organizations operate with two levels of sensitivity: level 1 and level 2.
As described in Table 51, the corpus of documents for each organization rarely makes explicit reference to the classification levels of the personnel or the IT systems those personnel have access to. With SME input and personal experience as well as on-line research, I differentiated the corpus-named IT systems by putting the correct classification domains on those systems. The agents (IT and Human) with the level 2 attribute set, have direct access to both levels of knowledge. Level 2 humans have access to both levels of IT systems, while level 2 systems will only be able to connect to other level 2 systems. Inter-connecting level 1 and level 2 systems does not happen in this dissertation, though future work could include such interconnections. The DoD calls such interconnections across classification domains cross domain solutions (CDS).

**IT systems’ capabilities and limitations for D2M and stylized organizational models**

In each type of model, IT systems are agents with different sets of limitations and capabilities than human agents. IT systems are, themselves, agents within the simulation, but they are able to communicate with more agents per turn in both send and receive mode. IT systems communicate more complex messages per turn than do human agents. IT Systems do not lie, and they rarely forget facts compared to human agents. IT systems do not have beliefs, and they can suffer from availability attacks where, even if present in the simulation, they are unable to communicate with other agents in the simulation until the attack is over.

**Shared planning, or operations order (OPORD), knowledge for D2M and stylized organizational models**

There is also, as part of the scenarios in use by the dissertation, a shared common set of ‘planning’ knowledge. These knowledge bits, shown below in Figure 121 as blue dots, have multiple links with red agents. The six (6) red agents in this particular figure are ‘Key IT’ systems in the classified and unclassified domains. These systems connect to the knowledge as well as provide interorganizational links to their peer systems in other organizations. The blue dots in the upper right corner of Figure 121 represent the starting configuration of a test run where only the singular Level 2 IT system per organization had access to all the plan data.
Inferring physical proximity for agents

Physical proximity, as well as the perceived difficulty of overcoming such distance (Conrath, 1973), is a well known mediator to communications. Construct uses physical proximity in its calculations of interaction probabilities on an agent x agent basis every turn. To support this use, Construct needed data. To generate data, especially in the near complete absence of geographical locations and distances in doctrine, it is necessary to apply additional data generating techniques. There were twelve steps to the process of calculating a physical proximity network.

Location by Location network with links as distance in kilometers

After down selecting nodes in the location node set, I created nodes for the approximate locations of each of the organizations and commands of interest. Google maps™ offered a fabulous opportunity to generate geospatial data independent of classified data sources. By adding latitude and longitude to each location, I was then able to export the data to Excel and calculate the pair-wise distance between all locations. I used the law of cosines to calculate the distances in kilometers using the equation below, and $\phi_1 = \text{latitude}_{\text{location A}}$, $\phi_2 = \text{latitude}_{\text{location B}}$, and $\Delta \lambda = \text{longitude}_{\text{location B}} - \text{longitude}_{\text{location A}}$ all in radians.

$$d = \cos^{-1}(\sin \phi_1 \times \sin \phi_2 + \cos \phi_1 \times \cos \phi_2 \times \cos(\Delta \lambda))$$

Equation 39 Law of Cosines to calculate distances between two points on a sphere

Creating a Agent x Location network, count of common organizations

The next step was to create a network of Agents by organizations where the link values are the counts of shared organizations. This will give me a denominator for calculating the
average distance across all same-agents at multiple organizations—in other words an agent George may be common to multiple organizations and this will generate the count of those shared organizations. Using previously discussed node set and matrix notations, the equation to generate this network is shown below.

\[ \mathbf{AL} = \mathbf{AO} \times \mathbf{OL} \]  
(42)

Equation 40 Generating an agent x location network (count of shared organization)

**Creating a Agent x Location network, sum of distances between egos**
The next step was to create a network of Agents by locations where the link values are the sums of distances across all the instances of each particular agent at each location.

\[ \mathbf{AL} = \mathbf{AL}_{\text{dichotomized}} \times \mathbf{LL} \]  
(43)

Equation 41 Generating an agent x location network (sum of distances between ego instances)

**Creating a Agent x Agent network, count of common locations**
The next step was to create a network of Agents by agents where the link values are the counts of shared locations.

\[ \mathbf{AA} = \mathbf{AL} \times \mathbf{AL}^T \]  
(44)

Equation 42 Generating an agent x agent network (count of shared locations)

**Creating a Agent x Agent network, sum of distances between egos and alters**
The next step was to create a network of Agents by agents where the link values are the sum of distances between each ego (row agents) and their alters (column agents). I use (43) to assist in calculating this value and show the equation below.

\[ \mathbf{AA} = \mathbf{AL}_{\text{dichotomized}} \times \mathbf{AL}^T \]  
(45)

Equation 43 Generating an agent x agent (sum of distances between egos and alters)

**Cell-wise division to generate average distance between egos and alters**
The next step is to generate the average distance, by dividing each cell of (45) by the sum of the respective cell in (44) and the row sum of the ego in the agent x location network. This is more easily depicted in the equation below.
\[ A_{\text{physical proximity}} = \frac{A_i A_j \text{sum of ego-to-alter distances}}{A_i A_j \text{shared loc count} + A_j ||_\text{row count}} \]  

Equation 44 Generating average distance between ego and alter agents

**Cell-wise inversion and return to ORA™ the agent x agent physical proximity network**

The last step in generating the physical proximity network, where the links represent the average distance between egos and alters, is to cell-wise invert the values to achieve the scale Construct expectes of \([1.0,0]\), for maximally close and maximally distant.

\[ A_i A_j = \begin{cases} 1, & \text{if } i = j \\ \frac{1}{A_i A_j}, & \text{otherwise} \end{cases} \]  

Equation 45 Generating an agent x agent physical proximity network for use by Construct, scale \([1.0,0.0]\)

With the copying of the results of (47) back into ORA as a network called ‘physical proximity’ the modeler has provided Construct with the data to computer the physical proximity component of interaction probabilities between agents.

**Experimental Setup**

As previously discussed, there are two tracts within this dissertation: a text mined modeling tract and a stylized modeling track. For each tract, I put under test various combinations of cyber effects (i.e., confidentiality, integrity, availability) targeting specific IT systems or more general communications mediums. The intent of the experiments was to judge if the graphical representations of resilience of measures of interest (MoI) (Figure 2) were theories with empirical foundations and to what degree. Additionally, the expectations of the experiment were to fulfill another deliverable of the dissertation, a rapid multi-dimensional assessment of resilience of organizational models that were themselves rapid constructions from self-documentation. Finally, two broad categories of mitigations were put under test: functional changes and organization structure changes, operationalize as new arrival training, spare/replicas of Key IT systems and procedures for bringing them on-line, and changing the ratio of meetings to planning sessions.
New arrival training informs new members of the organization who-knows-what and who-does-what. These correspond exactly with Construct’s ability to implement knowledge transactive memory and task assignment transactive memory. New arrival training has a history of improving organizational performance (Bartel, 1994) with Tracey et al building the General Training Climate Scale to provide feedback to management (Tracey & Tews, 2005). Within the military, this is akin to a new arrival receiving an overview briefing of the organization with fairly explicit details about what each staff section and sub-section does, as well as learning the names of members in those sections. Learning what the sections do (task assignments) supports individual agents in creating generalized perceptions of all agents in the subsections. By varying the false positive rates and false negative rates for each of the types of perceptions, I expect the modeled organizations to have better performance with low false rates for all four variables.

The second change, use of replica Key IT systems (and their starting knowledge) and varying how fast the equipment is brought online, increases knowledge redundancy within the organization. Redundancy as a means of improving resilience to disruptions is a known technique in multiple fields: public-key cryptosystems (Frankel, Gemmell, Mackenzie, & Yung, 1997), design of control systems in critical infrastructures (Rieger, Gertman, & McQueen, 2009), provision of public services (Low, Ostrom, Simon, & Wilson, 2003), and is frequently seen in functional redundancies in ecosystems (Low et al., 2003). The US Chemical Safety and Hazard Investigation Board (Crichton et al., 2009) widespread distribution of knowledge, especially of past organizational failures, is specifically called out by. The variable aspect of this component is how fast mitigation techniques are fully in effect—analogous to rehearsals that improve the ability of organizations to react to situations.

The last mitigation I experiment with, is the varying of the meeting to planning ratio for the JPG and JPG briefing attendees. In time compressed environments, the military already practices something like this mitigation—it is sometimes called an abbreviated military decision making process. Abbreviated MDMPs usually require more participation by leaders (more ‘meetings’ or larger audiences) and less time by specialized planners (JPG planning) isolated in their planning cell. Changing meeting time ratios and attendees are both techniques common in the emergency management services (Comfort, 2006). I expected modeled organizations with this mitigation to have better performance than the baseline up to a point, and then I expect a worsening return on investment of leaders’ time.
The verbiage of the variables placed under test can get daunting. In addition to the explanations above, I offer two additional aids: a graphical rendering of the factorial tree of categorical variables with Box-Behnken leaves, and a set of tables.

![Graphical rendering of experimental setup with factor tree and Box-Behnken leaves](image)

- **Categorical vars** (blue shades) populate a full factorial tree
- **Quantitative vars** (orange) populate leaves of the tree using Box-Behnken designs for Response Surface Modeling

Figure 122 Graphical rendering of experimental setup with factor tree and Box-Behnken leaves

<table>
<thead>
<tr>
<th>Condition</th>
<th>Possible Values</th>
<th>Quant. Combos</th>
<th>Cat. Combos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Model</td>
<td>Strategic, Operational</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Confidentiality Attack (IT)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Integrity Attack (IT)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Availability Attack (IT)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Availability Attack (email)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Availability Attack (phone)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Availability Attack (web)</td>
<td>$P_{\text{effect}}=0.0,0.2,0.8$</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td><strong>Mitigations:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge tm false positive rate</td>
<td>$P_{\text{effect}}=0.2,0.1, 0.05$</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
A naïve implementation of the experimental table above would yield a factorial result shown below. Clearly this is an infeasible number of iterations especially given runs times of 1 - 5 minutes per turn, even across a high throughput computing cluster.

\[
\begin{align*}
2 \text{ models} \times \frac{3^{10}}{\text{model}} \times \frac{20}{\text{combination}} = 7,085,880 \text{ iterations} \\
\end{align*}
\]

(48)

After equation 46, Naive experimental summary

Instead of planning on a naïve implementation as shown in (48), I turned to the Box-Behnken designs for response surface modeling (RSM) (Box & Behnken, 1960). The 10 factor design, called ‘Design 7’ in the above looks like the table below, where ±1 indicates to the modeler to take the top and bottom values of the three specified values for that variable.

<table>
<thead>
<tr>
<th>Knowledge tm false negative rate</th>
<th>( P_{\text{effect}} = 0.2, 0.1, 0.05 )</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task tm false positive rate</td>
<td>( P_{\text{effect}} = 0.2, 0.1, 0.05 )</td>
<td>3</td>
</tr>
<tr>
<td>Task tm false positive rate</td>
<td>( P_{\text{effect}} = 0.2, 0.1, 0.05 )</td>
<td>3</td>
</tr>
<tr>
<td>Speed of Mitigation in Plan-Brief Cycles</td>
<td>0, 1, 3</td>
<td>3</td>
</tr>
<tr>
<td>Meeting-Plan Ratio</td>
<td>0.20, 0.40, 0.60</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 53 10 factor Box-Behnken design

<table>
<thead>
<tr>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
<th>Factor 6</th>
<th>Factor 7</th>
<th>Factor 8</th>
<th>Factor 9</th>
<th>Factor 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
</tr>
<tr>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>±1</td>
</tr>
<tr>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
</tr>
<tr>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
</tr>
<tr>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>0</td>
</tr>
<tr>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
</tr>
<tr>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>±1</td>
<td>±1</td>
<td>0</td>
<td>±1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Expanding Table 53 and including ten (10) iterations of the last combination (the baseline condition), this RSM technique allows me to reduce the number of iteration substantially. The final number of combinations per model is 179, yielding the equation below for the number of iterations within the experimental design.

\[
2 \text{ models} \times \frac{179 \text{ combinations}}{\text{model}} \times \frac{20 \text{ iterations}}{\text{combination}} = 71,600 \text{ iterations}
\]  (49)
Simulations

The simulations for this dissertation use Construct, the agent based model simulation discussed at length in the Overview of Construct section that started on page 165. Revisiting the dissertation workflow from Figure 36, we can see where we are in the dissertation workflow by looking at the colored ovals and box in Figure 118.

Before describing the uses to which I put Construct, it is appropriate to discuss some of the changes I put in place, the testing for verification and validation of the changes, and the support I built in for continued maintenance and updates.

Changes to Construct

Construct began in the late 1990s, and has been modified extensively since then by researchers in CASOS and CASOS alumni now at other research institutions. Even with those changes, there continue to be modifications in the code base for purposes of resolving usability issues, aligning user documentation with as implemented functional, adjusting as-designed documentation to reflect as-implemented as well as the reverse. To use Construct for my purposes, to conduct Rapid Mission Assurance Assessment via Sociotechnical Modeling and Simulation, I needed some additional functionality that I have briefly alluded to in previous chapters.
Code base descriptives

When assessing code base complexity, a long-standing, but somewhat simplistic measure of complexity is the lines of code (LOC) in the project. Table 54 below depicts the descriptives created by cloc, a perl application (Danial, 2015) of the source code before I and other CASOS developers began modifying it in 2012.

<table>
<thead>
<tr>
<th>Language</th>
<th>files</th>
<th>blank lines</th>
<th>comment lines</th>
<th>code lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>C++</td>
<td>71</td>
<td>9,355</td>
<td>14,166</td>
<td>27,519</td>
</tr>
<tr>
<td>C/C++ Header</td>
<td>80</td>
<td>4,164</td>
<td>3,615</td>
<td>12,960</td>
</tr>
<tr>
<td>CMakel</td>
<td>2</td>
<td>472</td>
<td>310</td>
<td>1,605</td>
</tr>
<tr>
<td><strong>Sum:</strong></td>
<td>154</td>
<td>14,022</td>
<td>18,097</td>
<td>42,187</td>
</tr>
<tr>
<td><strong>Total LOC</strong></td>
<td>74,460</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A second table, Table 55, depicts the combined efforts of source code modification between three authors. My classmate Kenny Joseph is responsible for implementing the Boolean Transactive Memory related modifications to the application. A simple line count for those efforts are included, and then deducted from the total changes observed in the code base.

<table>
<thead>
<tr>
<th>Language</th>
<th>files</th>
<th>blank lines</th>
<th>comment lines</th>
<th>code lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>XML (testing input files)</td>
<td>8</td>
<td>622</td>
<td>891</td>
<td>45,769</td>
</tr>
<tr>
<td>C++</td>
<td>161</td>
<td>9,549</td>
<td>18,469</td>
<td>31,634</td>
</tr>
<tr>
<td>C/C++ Header</td>
<td>172</td>
<td>5,128</td>
<td>5,817</td>
<td>18,854</td>
</tr>
<tr>
<td>CMakel</td>
<td>3</td>
<td>35</td>
<td>82</td>
<td>115</td>
</tr>
<tr>
<td>DOS Batch</td>
<td>2</td>
<td>36</td>
<td>9</td>
<td>116</td>
</tr>
<tr>
<td><strong>SUM:</strong></td>
<td>346</td>
<td>15,370</td>
<td>25,268</td>
<td>96,488</td>
</tr>
<tr>
<td><strong>Total LOC</strong></td>
<td>50,719</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total LOC Change</strong></td>
<td>8,532</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TMBool LOC</strong></td>
<td>2,536</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LOC Change w/o TMBool</strong></td>
<td>5,996</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I was unable to differentiate Mike Kowalchuck’s work as it was throughout the code base. Mike is one the principal staff developers in CASOS, and he had the yeoman’s task of incorporating all the many changes Kenny and I created. The changes, grossly summarized in terms of lines added, or removed, are shown below in Table 56. Of note in this table is the im
Table 56 Lines of code added and removed during refactoring and additions

<table>
<thead>
<tr>
<th>Language</th>
<th>files</th>
<th>blank</th>
<th>comment</th>
<th>code</th>
</tr>
</thead>
<tbody>
<tr>
<td>make</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>removed</td>
<td>1</td>
<td>439</td>
<td>244</td>
<td>1,276</td>
</tr>
<tr>
<td>Bash Shell</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Added</td>
<td>1</td>
<td>33</td>
<td>9</td>
<td>113</td>
</tr>
<tr>
<td>removed</td>
<td>1</td>
<td>31</td>
<td>6</td>
<td>103</td>
</tr>
<tr>
<td>DOS Batch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>removed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>XML</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>8</td>
<td>622</td>
<td>891</td>
<td>45,769</td>
</tr>
<tr>
<td>removed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>C++</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>161</td>
<td>9,549</td>
<td>18,469</td>
<td>31,634</td>
</tr>
<tr>
<td>removed</td>
<td>71</td>
<td>9,355</td>
<td>14,166</td>
<td>27,519</td>
</tr>
<tr>
<td>C/C++ Header</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>172</td>
<td>5,128</td>
<td>5,817</td>
<td>18,854</td>
</tr>
<tr>
<td>removed</td>
<td>80</td>
<td>4,164</td>
<td>3,615</td>
<td>12,960</td>
</tr>
<tr>
<td>HTML</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>821</td>
</tr>
<tr>
<td>removed</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CMake</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>same</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>modified</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>added</td>
<td>3</td>
<td>35</td>
<td>82</td>
<td>115</td>
</tr>
</tbody>
</table>

191
The changes I brought to the code base involved extending Kenny’s code to be used for binary tasks as well as binary representations of transactive memory. I added copious quantities of embedded and inline comments and explanations using the comments geared for ingestion by doxygen €van Heesch, 2014 #7682¥, a program that creates source code documentation and graphical class inheritance diagrams in multiple output formats. The majority of the files I added to the source base fell into one of two categories: unit test files and refactoring classes into their own files (in lieu of multiple classes in a single header/source file pair). The end state of the dissertation is that I have placed 23 classed under varying levels of test coverage, ranging from 100% to as little as 10% of the public APIs. The principle advantage to this contribution is that future developers can use both the Boost Unit Test Framework test cases and the XML input files from previous versions to verify their implementations perform as they should and as the older versions of Construct used to.

| removed | 1 | 33 | 66 | 329 |
| SUM: | | | | |
| same | 0 | 0 | 0 | 0 |
| modified | 0 | 0 | 0 | 0 |
| added | 350 | 15,370 | 25,268 | 97,309 |
| removed | 154 | 14,022 | 18,097 | 42,187 |

The changes I brought to the code base involved extending Kenny’s code to be used for binary tasks as well as binary representations of transactive memory. I added copious quantities of embedded and inline comments and explanations using the comments geared for ingestion by doxygen €van Heesch, 2014 #7682¥, a program that creates source code documentation and graphical class inheritance diagrams in multiple output formats. The majority of the files I added to the source base fell into one of two categories: unit test files and refactoring classes into their own files (in lieu of multiple classes in a single header/source file pair). The end state of the dissertation is that I have placed 23 classed under varying levels of test coverage, ranging from 100% to as little as 10% of the public APIs. The principle advantage to this contribution is that future developers can use both the Boost Unit Test Framework test cases and the XML input files from previous versions to verify their implementations perform as they should and as the older versions of Construct used to.

<table>
<thead>
<tr>
<th>Table 57 Class count changes in code base</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Code base stage</strong></td>
</tr>
<tr>
<td>Pre-Dissertation</td>
</tr>
<tr>
<td>Post-Dissertation</td>
</tr>
<tr>
<td>Class growth</td>
</tr>
<tr>
<td>Unit Test Classes</td>
</tr>
</tbody>
</table>

**Baseline Analysis**

To establish the experimental baseline, and after conducting the augmentation of the model as I discussed in the previous chapter, I used the CASOS Condor High Throughput
Computing Cluster. This cluster supported executing multiple iterations per run condition to identify inherent variability in the execution of the model. The variability helps establish face validity in the minds of reviewers as it demonstrates the ability to incorporate stochastic processes into the simulation.

The baseline analysis of the simulations does not directly include the newly developed resilience measure. This is principally because in test and initial simulations, there were observed effects on the measure. Part of the no change result was predicted, as I don’t use resources in the Construct model, even though I use them in the static assessment model. I had expected some change however since the attack scenarios involve the logical deletion of highly connected agent nodes. I expected this would cause the creation of pendants of pendants in the agent chains remaining in the model. I had also expected knowledge bits connected to the deleted agents would contribute to a change in the resilience score. I was wrong. What changes did occur happened in the four and fifth decimal places, and I had to revisit my expectations.

My working hypothesis for this outcome is that the process of augmenting the model for Construct caused the agent node pendants of pendants to no longer exist. Addition of links and joining agents to groups caused them to not be isolated anymore. As to knowledge, if there were any knowledge bits that could no longer diffuse when the availability attack occurred, its loss was not noticed by the organization level measures. Finally, when augmenting and cleaning the data file, especially in an my efforts to reduce run times to a manageable duration, I use an automated remove isolates capability in ORA. Because I defined isolates using the entire meta-network ontology, there were still several thousand knowledge bits in the ORA model, not connected to a single agent, though many did form knowledge clusters. Without connections to agents, the knowledge bits were simply causing the simulation to run slower but still could never diffuse. This was also true of tasks. When I deleted isolates from those two individual networks (agent x knowledge and task x knowledge), I made it even more challenging for the resilience score to change. Given the lack of changes, my conclusion for the resilience score is I have demonstrated its applicability to static models generated from the D2M process. I have also demonstrated that model cleaning and augmentation techniques as well as attack scenario implementations can negatively impact the resilience score calculations.
Instead, I choose to analyze other aspects of performance that help answer the ‘so what’ of the indicated drop in performance we saw in the static analysis. In the static analysis chapter, we saw drops in measures that varied from nearly zero percent change to 60% and higher. To operationalize the impacts of those measures, the analysis deliberately constrains itself to the impacts to a small sub-set of the simulation population per model. Specifically, I focus on the diffusion of ‘plan’ knowledge in a normal execution environment to the agents that ‘attend’ the planning and plan briefing events in the simulation. An additional operating premise of the dissertation is that sufficient diffusion of ‘plan’ knowledge within key leader population is necessary for adequate execution of the plan. This premise nests with the generalized statement that the operational and strategic levels, commands tend to be more information-task oriented than other types of DoD organizations. The structure of my experiments, and the scenario that I have chosen is simply one instance of the many ways future researchers could instantiation a mission assurance simulation scenario.

In each of the two models, as shown in Figure 124 and Figure 125, the diffusion curves of the plan knowledge have the warm up period on the left of the chart, there is a increase in the rate of diffusion during and after each of the 3 simulated planning meetings. As noted in the augmentation chapter and even in the visual rendering of resilience from Figure 2, the warm up assist in establishing an equilibrium with respect to agents transactive memory being initialized and stabilized, stereotypes generated, and entropy associated with forgetting.

![Figure 124 Baseline 'plan' diffusion for operational model](image)
The graphs also demonstrate that in non-contested simulated environments, these organizations are completely capable of diffusing plan knowledge. There is also good evidence in Error! Not a valid bookmark self-reference. and Figure 127 that the D2M harvested knowledge-based tasks demonstrate high performance as accuracy measures. This measure, applied to each model in turn, has as its operating premise that alignment of agent-possessed knowledge to task-required knowledge leads to increased probability of high performance. The caveat of course is the measure does not offer task-specific visibility to leaders about which tasks, per-se, the organization will do poorly in, it simply offers an indicator of increased probability of higher or lower performance.

From this baseline analysis of non-contested environments, I move on to analyzing and summarizing the six attacks in their various combinations as well as the mitigations. Before doing so, I will provide a slightly more in-depth review of the mitigations in place.

Mitigations

New arrival training informs new members of the organization who-knows-what and who-does-what. These correspond exactly with Construct’s ability to implement knowledge transactive memory and task assignment transactive memory. New arrival training has a history of improving organizational performance (Bartel, 1994) with Tracey et al building the General Training Climate Scale to provide feedback to management (Tracey & Tews, 2005). Within the military, this is akin to a new arrival receiving an overview briefing of the organization with fairly explicit details about what each staff section and sub-section does, as well as learning the names of members in those sections. Learning what the sections do (task assignments) supports individual agents in creating generalized perceptions of all agents in the subsections. By varying
the false positive rates and false negative rates for each of the types of perceptions, I expect the modeled organizations to have better performance with low false rates for all four variables.

The second change, use of replica Key IT systems (and their starting knowledge) and varying how fast the equipment is brought online, increases knowledge redundancy within the organization. Redundancy as a means of improving resilience to disruptions is a known technique in multiple fields: public-key cryptosystems (Frankel et al., 1997), design of control systems in critical infrastructures (Rieger et al., 2009), provision of public services (Low et al., 2003), and is frequently seen in functional redundancies in ecosystems (Low et al., 2003). The US Chemical Safety and Hazard Investigation Board (Crichton et al., 2009) widespread distribution of knowledge, especially of past organizational failures, is specifically called out by. The variable aspect of this component is how fast mitigation techniques are fully in effect—analogous to rehearsals that improve the ability of organizations to react to situations.

The last mitigation I experiment with is the varying of the meeting to planning ratio for the JPG and JPG briefing attendees. In time compressed environments, the military already practices something like this mitigation—it is sometimes called an abbreviated military decision making process. Abbreviated MDMPs usually require more participation by leaders (more ‘meetings’) and less time by specialized planners (JPG planning) isolated in their planning cell. increasing shared situation awareness. This technique is also common in the emergency management services (Comfort, 2006). I expected modeled organizations with this mitigation to have better performance than the baseline up to a point, and then I expect a worsening return on investment of leaders’ time.

**Strategic Model**

As previous work (Lanham, 2011) indicated, I had expected that the strategic model would experience non-linear changes when confronted with multiple attack vectors. In the series of figures below (though by no means a comprehensive set of all 179 conditions), the reader can see there is a dramatic effect in the decreased performance during and immediately after the attack.

![Figure 128 Strategic model linear effects for single-vector attack conditions](image)

![Figure 129 Strategic model non-linear effects for multi-vector attack conditions](image)
I had expected the mitigation of reducing the transactive memory error rates would provide a more substantial effect on plan knowledge diffusion that it demonstrated below in Figure 130. With a decreased opportunity to have incorrect perceptions, the simulation suggests that newcomer training is helpful in increasing diffusion, even in contested cyber environments. This suggests to commanders that should emphasize initial who-does-what and who-knows-what, at least in the larger organizational sub-groups.

![Figure 130 Strategic model with newcomer training modeled as a reduction in transactive memory error rates](image1)

What I had not expected was the rather dramatic rise in plan diffusion after attacks in the scenarios where the spares were brought online. As seen in Figure 131, the plan diffusion curve is a definite improvement to the no attack condition as well as the pre-attack condition. My working hypothesis, and in retrospect predictable outcome, is that there is simply more IT systems with the plan knowledge in these scenarios, thereby helping spread the information at a faster rate and to a larger population.

![Figure 131 Strategic model with post-event diffusion better with spares than in the baseline condition.](image2)

I had expected and saw an increase in plan diffusion by changing the ratio of meeting time to planning time during the planning cycle. Though the increase is not dramatic, this particular adaptation has operational challenges in units. What it effectively does is requires a large percentage of key leaders in the organization to decrease their attention and effort spent on their other duties. This worked fine in this scenario, but would likely cause many a commander to have second thoughts on doing so as a long term solution.

**Operational Model**

Like the strategic model, the operational model experiences non-linear changes when confronted with multiple attack vectors. The figures that follow convey to the reader there is an effect, though less dramatic than the drop for the strategic model, in the decreased performance during and immediately after the attack.

![Figure 132 Operational model linear effects for single-vector attack conditions](image3)

![Figure 133 Operational model non-linear effects for multi-vector attack conditions](image4)
Like the strategic model, I had expected the mitigation of reducing the transactive memory error rates to provide a more substantial effect on plan knowledge diffusion that it demonstrated below in Figure 134. With a decreased opportunity to have incorrect perceptions, the simulation suggests that newcomer training is helpful in increasing diffusion, even in contested cyber environments. This suggests to commanders that should emphasize initial who-does-what and who-knows-what, at least in the larger organizational sub-groups.

Figure 134 Operational model with newcomer training modeled as a reduction in transactive memory error rates

The dramatic rise in plan diffusion after attacks in the scenarios where the spares were brought online was less pronounced in the operational model than it was in the strategic model. As seen in Figure 135, the plan diffusion curve is an improvement to the no attack condition for strategic scenarios as well as the pre-attack condition. My working hypothesis remains the same; there are more IT systems with the plan knowledge in these scenarios, thereby helping spread the information at a faster rate and to a larger population.

Figure 135 Operational model with post-event diffusion better with spares than in the baseline condition.

I had expected and saw an increase in plan diffusion by changing the ratio of meeting time to planning time during the planning cycle. Though the increase is not dramatic, this particular adaptation has challenges in operational units as it does in strategic units.

The 10 dimensional response surface generated by the Box-Behnken design shown in Table 53 is necessarily inaccessible for visual rendering except in slices and pieces. I have not depicted or discussed outcomes for combinations of factors that do not demonstrate outcomes of potential interest to organizational leaders. This is a useful aspect of M&S based experimentation however as there are little to no differential costs in running additional scenarios—though the same is not true of the analysis efforts associated with each scenario. What this approach supports however is forecasting for conditions that will, or should, cross the risk-acceptance thresholds of organizational leaders. Those leaders can use the scenarios with intriguing or obvious results to guide their decisions to establish training objectives and expectations in their formal training calendars and events. The outcomes of the M&S experiments thus serve as screen criteria for selecting high-payoff scenarios when the unit shifts from simulation to live or constructive training modalities.
Heuristics

This chapter is an opening effort at distilling tens of pages of detailed analysis to heuristics for consumption by organizational leaders. Like all heuristics, their value will come from their general accuracy, their brevity, their references to other experiential frames of references, and their adoption. Some of the heuristics below are not directly supported by the evidence of this dissertation, but are extrapolations of experience and intuition. The very need for extrapolation is evidence of the continuing gaps in research and experiential learning.

First and foremost, to paraphrase a co-worker, military cyber space operations are traditional military operations on non-traditional terrain (Lanham, 2012a). Removing the military context, cyber space operations are traditional business operations in non-traditional regulatory and market environments. Moderately stripping away the aura of uniqueness and specialness of the IT-realm can enable leaders to recall their other professional planning and coping skills while avoid the pitfalls of disaster mythologies (Tierney et al., 2006). This rule of thumb is especially important and seen in practice during community reactions to natural disasters (Coping with Catastrophe: Building an Emergency Management System to Meet People's Needs in Natural and Mammade Disasters, 1993; Quarantelli, 1988; Reason, 1991): leaders that retain a semblance of calm under stress help the community maintain its sense of capacity to overcome adversity. In the military context, there are few scenarios where professional militaries will surrender or otherwise stop military operations simply because of setbacks and adversity nor would they tolerate leaders who refuse to plan and rehearse for obvious eventualities.

Legal authorities matter, as they do in traditional military and business operations. Espionage and warfare are lawfully different activities; as a nation, we do not habitually use the military to conduct espionage, nor do we use espionage agents to conduct combined arms military operations. Conducting everyday business and industrial espionage, sabotage, or counter-sabotage are also all different activities, controlled by differing legal frameworks, regardless of individuals personal opinions or beliefs. Combining these two heuristics leads to the following logical assessment. Military cyberspace operations are not inherently extensions of cyberspace espionage any more than coalition and multi-service maneuver and clash of armed forces are inherently extensions of covert operations.
Small well chosen targeted system losses can affect organizations as greatly as large random losses. Effects vary greatly by system(s) and duration of event(s)/outage(s). Of the twenty MoIs presented in the Entropic and Targeted Attacks starting on page 145, percentage change impacts were as low as 0-1% at 10% loss levels (random) to as high as 80% at 75% loss levels. Those percentage change can be a gross form of impact assessment, short of specific organizational impacts with SME-input (or experience), it remains a useful data point for leadership. With those caveats, the table below summarizes the impacts of random losses. The table is akin to the green, amber, red, black color coding schemes traditional military commanders use for assessing overall operational capability of an organization (see also Figure 117).

Table 58 Effects of random losses table

<table>
<thead>
<tr>
<th>Random Loss Level</th>
<th>Operational Impact for Organizational Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 15% random loss of IT agents and IT resources</td>
<td>Little to no operational impact on the 20 assessed SNA measures.</td>
</tr>
<tr>
<td>Up to 30% random loss of IT agents and IT resources</td>
<td>10% change threshold crossed on some of the 20 assessed SNA measures</td>
</tr>
<tr>
<td>Up to 50% random loss of IT agents and IT resource</td>
<td>Changes are highly variable and range from little to no impact to changes up 60% on the 20 assessed SNA measures</td>
</tr>
<tr>
<td>Up to 75% random loss of IT agents and IT resource</td>
<td>Changes are highly variable and range from moderate (&gt;10%) to severe impacts on the 20 assessed SNA measures</td>
</tr>
</tbody>
</table>

A more nuanced heuristic for the above table is that ‘it depends’ on the MoI, the effected system(s) and the operational impacts. For a hospital, the degradation of a centralized patient database, with no spares or failover capability, could dramatically effect sustained care while the health care providers revert to paper-based systems. The decision to revert would clearly be driven by an estimated time for return to service as well as assessments for any data integrity loss (e.g., corruption of patient data). For time sensitive targeting, organizations may lose small windows of opportunity (Pflanz & Levis, 2012), causing a reversion to other processes or other expectations. For strategic and operational logistics, degradations to business-to-business communications with commercial shipping, rail, and trucking companies may prove inconsequential for short duration events, and could impact controlled supply rates and restricted supply rates for specific classes of supply.
The table above is table, and the more nuanced answer are both aligned with the first paragraph of this chapter. A traditional military commander at the operational level would have an experiential and intuitive basis for knowing that a random loss of 15% of her aircraft may be very consequential of the 15% overlaps completely with a high value airframe. Or the logistician that understands the random loss of the sole material handling equipment at an airfield has ripple effects larger than a single piece of equipment loss would usually generate. Traditional business and military operations require risk mitigation, as does cyber space operations. Traditional military studies also strongly alternate, contingency, and emergency plans as well as rehearsals of the switch over and execution of those plans.

There is danger is assuming that resilience to everyday outages and challenges equates to resilience to deliberately contested cyber environments. The specific targeting of systems by a malicious adversary will be attempting to create effects within the targeted organization’s operations, leadership decision cycles, information flow, or some other goal. The research shows that combinations of key node losses can rapidly shift to non-linear effects disproportionate to the number of systems directly affected. In these models, deletion of as few as ten (10) nodes, when carefully selected, can create effects as large as a random loss of 50% of the nodes. For strategic and national level commands, who perceive themselves as reliant on up-to-the-minute information flow to make decisions, this argues that they should prepare for and rehearse degraded communications!

The paragraph above reinforces the first takeaway of the dissertation yet again. Traditional military operations seek to identify and target adversaries’ centers of gravity and decisive points. Such targeting helps set the stage of cascading successes by the friendly elements while depriving the adversaries of decision space and time. The loss of key leaders in an organization can have a disproportionate effect on the workers and processes. Likewise, the creation of an effect in a key leader’s world view, can dramatically affect the organization—a deliberate injection of erroneous data to a key leader or key IT system can rapidly and persistently corrupt the decision making and processes within an organization.

The clearest example of this degraded information flow is in Figure 110. An adversary can, in these models, double the amount of time it takes for information to flow through the organizational models. In this figure of these two models, the loss of a single IT system can
degrade communications flow up to 10%. Deliberate targeting by an adversary of just 10 IT centers of gravity can degrade IT-only diffusion by 50%, hence the doubling of time to move information. That time lag may be without effect, or it may place national decision maker(s) well outside their comfort zone for decisions without up-to-the-minute current data or information. Expectation management for impacts pre- and post-event is essential to ensure leadership demonstrates resilience in the face of an information addictions not receiving their periodic updates.

The table below reduces the content further with the commiserate risk of over simplifying and under stating the variability of outcomes.

Table 59 Rules of thumb for impacts

<table>
<thead>
<tr>
<th>Cyber Condition</th>
<th>Operational Impact for Organizational Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random and everyday losses != targeted or deliberate losses</td>
<td>Extrapolating from everyday random losses and typical troubles of ‘build, operate, and maintain’ mission to a malicious adversary imperils assurances as there is no confidence in coping plans</td>
</tr>
<tr>
<td>Contested cyber environments will happen</td>
<td>Org leaders and members having estimates of impacts avoids disaster myths, knowing how to adapt and approximate path for return to normalcy is essential to mission assurance</td>
</tr>
<tr>
<td>Up to 15% random loss of IT systems</td>
<td>Little to no operational impact—usually Akin to: if luck favors the adversary, loss of a main supply route</td>
</tr>
<tr>
<td>Up to 30% random loss of IT systems or Loss of a single ‘key’ IT system</td>
<td>Slight operational impact—dependent on which 30% of the population is affected Akin to: Loss of high level ‘key leader’ contingency requires succession of command plan and expectation of resilience</td>
</tr>
<tr>
<td>Up to 50% random loss of IT systems or Loss of up to four (4) ‘key’ IT systems</td>
<td>Moderate to severe impacts without Primary, Alternate, Contingency, and Emergency (PACE) plans in place and rehearsed. Impacts are highly variable! Akin to: Loss of an entire command group or other cluster of key personnel or resources.</td>
</tr>
<tr>
<td>Up to 75% random loss of IT systems or Loss of up to ten (10) ‘key’ IT systems</td>
<td>Moderate to severe impacts PACE plans in place and rehearsed. Akin to: Doubling time it takes to move reports across the organization(s). Loss of an forward airbase or port in...</td>
</tr>
</tbody>
</table>
The most important take away from this chapter is that the rapid modeling process of the previous chapter can generate a model subject to analytic efforts that demonstrates a recognizable, though nonunique, outcome: targeted removal of IT systems and IT resources in complex sociotechnical organizations can lead to effects disproportionate to the number of directly affected systems and resources. This trend leads to a lesson for organizational leaders that the risk management community has incorporated for a very long time: identify the most important systems and resources and ensure their continuity of operations at some a priori acceptable level. The decision process that identifies those important functions and capabilities can use the techniques in this dissertation as a mechanism, as well as supporting or supplemental means—the key is the realization that a few well-chosen losses will predictably have outsized impacts! This phenomenon has earned the moniker ‘black swan event’ in some circles though it is by no means the only descriptor.
Limitations and Future Work

Text-mining as basis of organizational modeling

There is clearly a prima fascia case for using documentation nominally describing an organization and its workings as the basis for constructing a model of the organization. Unfortunately, the relevant literature on organizational modeling does not address this technique on any consistent basis. This lack of discussion points to gap in applied research toward rapid model construction and a form of rapid model validation—a funding challenge compared to pursuing original theoretical research. The research questions currently open would be approximately, “Does mapping of concepts within sets to ontological categories create consistent meaningful distributions that support researchers’ efforts at validating the ‘accuracy’ of those mappings?” If the answer is yes, a follow-on question could be, “How small a corpus can an organization use to establish a defined confidence interval (e.g. 95th percentile) of capturing meaningful nodes?”

As alluded to in the Literature Review portion of this dissertation, starting on page 10, as well as the comparisons of edit-cycle 0 and terminal models generated in the D2M-process (see also Figure 37 and Figure 38), there is a current lack of empirical data for multi-domain ontological distributions. An approach to resolving this lack of empirical data is not hard to envision, and I look forward to pursuing such data in the future. I currently envision a detailed analysis of each input file across the chosen sets, with pre- and postcleaning collection of data, processing times, outputs, and pre- and postprocessing decisions. I foresee the output of interest being the distributions of the metanetwork ontology per megabyte of input. With those distributions, a future research could, with better mathematical certainty, assert their inputs are representative of the population, as well as their postcleaning results fall within a known standard-deviation from norms. Clearly the choice of ontology would impact the mapping and distributions of concepts to ontological categories. Unless and until sufficient empirical data is available across multiple domains, its infeasible to assert that the distributions evidenced in this dissertation reflect ‘truth.’

Limitations of doctrine and written products as the basis of models

Doctrine and other written products have several obvious shortcomings as the basis of models of specific organizations. Joint doctrine is authoritative within the DoD but is not
prescriptive. Organizations and leaders have the explicit leeway to deviate from doctrine—frequently causing doctrine to be a common point of departure. There is apocryphal story that an American adversary complained that studying American doctrine was useless, as the Americans do not read their own manuals or feel any obligation to follow their doctrine. Though it is a stretch to assert that doctrine is honored more in its being ignored than followed, it is also a stretch to assert that the DoD religiously adheres to its doctrine.

Organizations’ written documents can help reduce the disconnect between the way the organization writes about itself and any doctrine/documents that others write about it. Those written documents, depending on their nature, can also help reduce the disconnect between the present day (assuming the documents are of recent generation) and the time when the document was written.

Doctrine is also slow to change or evolve in response to current or perceived futures. Generally, it attempts to overcome this known trait through leveraging the ‘authoritative but not prescriptive’ caveat within the DoD. This slowness to change can contribute to perceptions that any model derived from doctrine will not be applicable to current-day environments and situations.

**Cyber effects vs. methods-of-attack**

This dissertation has not directly modeled the various technical or natural methods that can create a contested environment. Instead I have used the information assurance ontology of confidentiality, integrity, and availability. This means my models do not include a motivation by agents that cause problems nor do the organizations have a perception of cause on the part of their agents. Including a perception of cause, or motivation, is an area of organizational adaptation that is ripe for exploration and analysis—intuition suggests potentially different adaptations to nature-caused effects versus adversary-caused effects. There is also potentially different adaptations or mitigations for adversary-caused effects and the vagaries of modern technology—between a suspected human insider spy and a technology-fault leading to data corruption within a database.
Modeling and Simulations

Emotive responses by agents during events

In none of my scenarios, or even in Construct itself, do any of my agents experience any steady or rising level of ‘frustration’ when they are unable to interact with their first choice or discover their interaction has been obviated by the failure of a communication mechanism. It seems safe to assume that emotional reactions to natural-event driven disruptions will vary from those reactions to suspected or known hostile actions.

There is significant evidence that in communities that suffer natural disasters, the expectation of return to some level of normalcy is key to resilience—in the information deprived environments the seeds of maladaptive outcomes are sown.

Inclusion of more D2M-ontology categories into Construct

‘Beliefs’ from D2M ontology better carried into Construct

Related literature already exists to support the assessment that agents’ beliefs contribute to a sense of likeness, or homophily (M. McPherson et al., 2001; Ridgeway, 2006). The extension of Construct to include beliefs would open the possibility of studying belief-influenced behaviors. Of particular interest to me would be application of beliefs to compliance studies in cyber security. I have a strong intuition that rules without supporting beliefs in the rules’ efficacy or applicability are counter-productive to the end-states the rules had intended to achieve.

Compliance studies exist in a number of fields from sector specific EU studies (Börzel & Knoll, 2014), providing health care (Rydenfält, Ek, & Larsson, 2013), public administration and red tape (Bozeman & Feeney, 2011), but there appears to be a dearth of compliance studies related to cyber security and incorporating modeling and simulation. I am most interested in research questions that acknowledge humans are the biggest attack surface of any IT system, and whether and how influencing their behavior interacts with technology-focused security efforts.

‘Events’ from D2M ontology carried into Construct

Extending and expanding the forecasting abilities of Construct to a larger set of events would also be a very useful avenue of research. Forecasting future events, the possible impacts of those events on measures of interest, and organizational responses to those events is essential mission assurance as I depicted the concept in Figure 1.
It is not entirely clear to me whether the semantic concepts of events that the D2M process can harvest are translatable into forecastable events. But even if the D2M generated ‘event’ nodes are not good candidates for specific event modeling, there is a large set of possible events that could reasonably form a body of M&S researcher scenarios.

An alternative way of incorporating D2M harvested events is to use them and agents linked to them as drivers of shared-experience interactions. Such an extension to Construct might fall under the umbrella of trust building and interactions with trusted persons for human agents as well as supporting the ‘trustworthy’ belief between egos and alters.

‘Roles’ from D2M ontology carried into Construct

Modelers and researchers can already use Construct to model implicit roles such as boundary spanners, leadership at the top of hierarchies, and other structural definitions of roles. In this conceptualization, I am leaning more toward the differentiation humans give to our various professional and personal roles.

Professional roles within the DoD could be as broad as personnel categories (e.g., general officer, field grade officer, company grade officer) or as specific as work roles (e.g., chief of operations, executive assistant). These roles place implicit, and sometimes explicit, constraints and limitations on decisions by agents. In Construct as implemented, agents have no ability to perceive their roles nor the roles of other organizational members. The D2M process already captures some of the agent x agent links represented in these work specific roles. Having a M&S based implementation of one or more role-based behavior pattern generators would open the door for additional research about whether particular roles are more or less resilient to contested cyber space operations. It could also incorporate lessons from resilience studies of communities and community leadership to negative events (Norris et al., 2008).

A second way of potentially incorporating social roles into future work is incorporating the duality of at-work behavior and away-from-work behavior. This is a direct extension of the role discussion in the previous paragraph, as organizational members at work have different motivations for interacting with organizational members, than when they are away from work. Family and non-work social interactions, even if they share common motivations (e.g., homophily), the factors used to assess the homophily change—even if the resulting patterns do not.
‘Resources’ from D2M ontology carried into Construct

Task execution in Construct is accomplished in one of two ways: knowledge based decision making (e.g., binary classifications) or energy tasks (not used in this dissertation). Though it is not immediately apparent whether a bolt-on module could be added to Construct to incorporate resource-based tasks, it would certainly broaden the perception of face validity for organizations that conduct activities other than information sharing and processing. Such a bolt-on module would, ideally, be able to directly use the resources identified during the D2M process, as well as the linked nodes to those resources. Resource acquisition could then become its own motivator for interaction, as well as resource acquisition in pursuit of accomplishing resource based tasks.

Circadian rhythms carried into Construct for human agent interaction patterns

Circadian rhythm incorporation within Construct could conceivably assist modelers in developing more complex representations of organizations, should such rhythms be value added. It would require the concept of turns in Construct to become less broad in the general sense, and need to be a selectable option in any case. As currently implemented, each turn can represent as much or as little of real time the modeler assesses is appropriate. Modelers can also divorce real time and its passing from any overt representation in Construct models—an especially useful ability when there is too little empirical evidence to support initial configurations of rates of changes.

M&S is forecasting, not prediction

M&S of human populations can be and frequently is reflective of population level measures and trends. It is tempting to extrapolate that since the modeled populations reflect empirical populations, that modeled agents will reflect real-life agents. This extrapolation, though tempting, is unwise in the extreme. Construct is an excellent tool for group level interactions, trends, and supplying data to network analytic methods. Construct is not the right tool to model individual agents’ actions and reactions to their specific environments.

Fundamentally, this M&S as depicted in this dissertation is sufficient for forecasting results of meaningful use to organizational leaders. Construct-based M&S is not however appropriate to predict the actions and reactions of specific individuals.
Contributions

There are six contributions from this dissertation to the field of computational modeling of organizations and to organizational resilience as a component of organizational science. The first three are applicable directly to the study of resilience and the last three are technology-centric contributions that support resilience assessments.

The first contribution is a brand-new static measure of assessment within the theoretical structure of Dynamic Network Analysis (DNA) (e.g., multimode and multi-link graphic analysis). This was the function of resilience relating needs, redundancy, and near isolation to a final value.

The second contribution is a rapid process to generate mission assurance models for specific organizations. This process is responsive to leaders’ perceptions of ‘now’ and not weeks or months ago. It is also responsive to forecasting scenarios to help plan future resource commitment. This rapid process is through the application of SNA and DNA to mission assurance and resilience in contested cyber environments—unlike other state of the art cyber risk management techniques.

The third contribution is the incorporation of adaptive agents into mission assurance and resilience M&S. The majority of cyber risk management techniques do not incorporate the human element into organizational resilience M&S efforts. Supporting this contribution are the generalized assessments of resilience across multiple categorical and quantitative inputs of structure. Additionally, there are generalized assessments of resilience across multiple forms of contested cyber environments for baseline conditions and under mitigation efforts.

The three technology-centric contributions revolve around further refinements to the D2M-process under development at CASOS as well numerous technical updates, major and minor modifications to the Construct ABM simulation. Some of the modifications derived from extensive refactoring of code written by a multitude of developers over the years. Some were integration of automated code documentation tools with the code base and the incorporation of inline commenting and source-code level documentation. One of the larger major modifications was the initial development and use of test cases integrating a unit test framework. The unit test addition to the code base increases confidence that the fundamental function of the system remains consistent across the versions and years. Regression testing is a key benefit of the unit test add-ons.
Another substantial technological addition to Construct was implementing task transactive memory—an error prone and cognitively modeled perception by egos of tasks assigned to their alters within a simulation environment. Task-based homophily is now a capability that modelers can use, or not, based on the nature of their research and questions of interest. By adding this capability, modelers who desire to incorporate similarity of assigned tasks into agent behavior can do so.

The last technology-oriented contribution is a DoD-specific thesaurus suitable for continued use, reuse, and expansion within the DoD for the D2M process. Thesauri can represent an enormous psychological barrier to use as well as a resource barrier; not all organizations can afford to create a thesaurus for use just by themselves. By using the thesaurus developed for this dissertation, future DoD organizations can increase their confidence in D2M generated models as well as speed of development of those models.
References

References


Bonacich, P. (1972a). Factoring and weighting approaches to status scores and clique detection. *Journal of Mathematical Sociology, 2*, 113-120.


217


Information Assurance (IA) and Support to Computer Network Defense (CND), 6510.01F C.F.R. (2011).


Levitt, R. E., & Kunz, J. C. Design your Project Organization as Engineers Design Bridges CIFE Working Paper (pp. 21): Stanford University.


Thibodeau, P. (2010). Cyberattacks an 'existential threat' to U.S., FBI says


Appendix 1 Definitions

Central Definitions

Below is a small collection of definitions essential to the dissertation. The next section is an alphabetical section that contains other definitions taken from various sources. When using sources, I choose to use, in order of precedence, National standards bodies’ definitions (e.g., CNSS), Joint doctrine, Service Doctrine, and finally dictionary definitions.

Cyberspace

“A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. “(Joint Staff J7, 2010a)

There are a multitude of definitions of cyberspace, some of which go on to enumerate the types and quantities of people and organizations (e.g., owners, customers, criminals, script kiddies, organized crime syndicates, nation-states) as well as the various types and natures of equipment (e.g., telecommunications companies’ (TELCO) routers, undersea fiber-optic cables, points of presence, setste perimeter routers and firewalls, organizational terminals and other IT). Additionally, many computer and information security practitioners and researchers believe threat enumeration (e.g., hacktivists, espionage, military forces, and ‘advanced persistent threats’) is necessary; the nature of threat(s) are inputs into the decision process of resource allocation. Adhering to the base definition in established doctrine however retains a broader perspective on the problem than using additional descriptors.

This dissertation models various types of organizations that own, use, operate, maintain and defend internet-protocol (IP)-based communication networks as well as other forms of telecommunications IT to facilitate information exchange. It also uses stylized representations of computing systems (e.g., databases, servers, client terminals) without delving into the technical implementation of those systems, their protocols, or their inner-workings.

Contested Cyberspace

A human-built environment constantly, but irregularly, effected by people and natural processes that can, and do, negatively interfere with the designed and intended purpose of that environment.
Merriam-Webster defines ‘contested’ as the following:

*to make the subject of dispute, contention, or litigation (contested, 2013).*

As discussed earlier, this dissertation, as well as the generalized discussion of mission assurance and resilience, requires a slight broadening of the definition above. This change is necessary as natural causes can create the same effects of denial, degradation, and disruption on availability as human-driven disputation or contention—though I’ve not found a reasonable path that nature can use to inflect effects on integrity or confidentiality.

**Mission Assurance**

The plain English definition this dissertation will use is shown below:

*Mission assurance means having a level of confidence in the resilience of an organization, its ability to recover from or adjust to cyber events, along one or more measurable dimensions.*

The USAF developed a nondoctrinal definition of mission assurance that conveys its core intent that the USAF and its units can “fight through an attack” (Elder, 2008). Importantly, the decision makers that developed this approach were not information security (INFOSEC) or computer security (COMPUSEC) practitioners. These decision makers were operations generalists who, by long experience and exposure, have learned that the complex choreography of USAF’s many missions have a central core: successful execution of military operations. The situation is akin to the organizations (e.g., oil exploration) that have multiple subelements (e.g., HR, Finance, Logistics) that perform necessary, even critical functions, that are, fundamentally, not the primary raison d’être of the organization.

Within the USAF multi-dimensional approach, shown in Figure 136, INFOSEC and COMPUSEC practitioners will note the overall effort subsumes traditional definitions of information assurance (IA) and computer network defense (CND).

Figure 136 clearly links the technical components of cyber capabilities and infrastructures (lower left) with the traditional notions of physical security (lower right). It also links the systems (center orange triangle) with the people and organizations (upper right) that use those systems. This depiction helped USAF leadership accomplish two (2) simultaneous tasks. The first was to enlighten traditional leadership in multiple facets of mission assurance without overly technical vocabulary. The second, and as importantly, was to ensure traditional ‘cyber’
personnel remembered that cyber capabilities are a means to an end—that peoples’ and organizations’ missions must be resilient to contested cyber environments and leaders are assured of that resilience. This continued meaningful functioning in the face of adversity leads us to our next, related definition.

![Mission Assurance (CYBEROPS) “Fight Through the Attack”](image)

Figure 136 USAF Visual Depiction of Mission Assurance (Elder, 2008)

**Resilience**

Merriam-Webster defines ‘resilience’ as the following:

> “an ability to recover from or adjust to misfortune or change” (resilience, 2012)

The nature of the misfortune or change is of course necessary to any discussion of resilience. The nature of who or what is being resilient, to what degree they are resilient to the misfortune, and how long they can demonstrate resilience are also essential to any analysis, assessment, and discussion of resilience. This dissertation contains both static structural assessments of resilience as well as dynamic assessments of resilience as a function of other measures.

> “Contested cyber environments” helps scope the discussion to the type of misfortune or change, as does focusing solely on organizational resilience. A first impulse for many organizations concerning themselves with a ‘contested cyber environment’ is to leap to discussions of ‘bad people’ doing ‘bad things’ to the organizations’ computers and other IT resources. This initial impulse can also lead to follow-on questions, such as:
• To what degree do organizational subelements depend on their computers for their local needs? To what degree do local needs affect the organization-wide needs?
• Are the ‘bad people’ insiders to the organizations or outsiders?
• Are the ‘bad things’ malicious acts? Obviously nonmalicious acts? Somewhere in between? ‘Back-hoe’ attacks by road repair crews are generally not malicious while purposeful hacking generally is malicious. Self-infection with malware is generally insider carelessness leading to external exploitation, can be malicious, but intent is hard to trace or otherwise prove.
• Are off-site ‘bad things’ (e.g., power outages, telecommunications outages, solar-storms) considered part of a contested cyber environment? Are they considered at all when developing mission assurance plans and assessments for resilience to contested cyber environments?

From these examples, it’s possible to get a sense of a broad spectrum of events that can comprise a contested cyber environment. Indeed the spectrum of mechanisms of affect are so broad, it’s unlikely that any single model or simulation capability could adequately represent them. There is clearly value in exploring, via technically oriented modeling and simulation (M&S), specific effects by specific mechanisms in both general and specific situations. But exploring a broad spectrum of mechanisms and effects via such sampling is not the only method for researchers and organizational planners. Indeed, this dissertation has one goal of allowing such broad exploration without the per-attack mechanism details being present in the model—supporting generalization of impact assessments!

Since the dissertation is not exploring per-attack buffer overflows, cryptographic attacks, denial of service (DoS) or distributed DoS (DDoS) mechanisms, the reader is probably interested in knowing what the dissertation will explore. The briefest answer is that the dissertation explores the effects of these various mechanisms, without the mechanisms themselves having explicit representation. Using the CNSS’ now common acronym of confidentiality, integrity, and availability (CIA) (2010), it is feasible to consider the effects of nearly every form of computer network attack (CNA) disruption, degradation, denial, destruction (Joint Staff J7, 2010a) or deception (USAF, 2012)) within a contested cyber environment. A mechanism may create effects in one or more of these ontological categories, relieving the modeler and simulationist from the need to simulation specific technical mechanisms and specific technical effects, and instead recreate these primary effects within the IA ontology of confidentiality, integrity, and availability.
Like (Pflanz, 2012; Pflanz & Levis, 2012) a visual chart depicting the dynamic nature of resilience is useful to convey a more complete understanding.

In this picture, there is the span of time from $t_0$ to $t_{\text{warmup}}$ that reflects the possible values of an MoI prior to reaching a pre-contested-environment equilibrium. As noted by Pimm (1984), without equilibrium, resilience is indefinable. During the time of normal operations ($\text{MoI}_{\text{normal}}$), there could be variance from the normal, though such variance over time would still need to establish equilibrium within some tolerances. The figure also depicts the beginning of an attack ($t_{\text{attack-start}}$), or some other form of cause for one of the CIA effects. While the attack is on going, the attack should be having some effect on the MoI, though it may not be consistent, statistically or operationally significant. As shown, there is an approximate stair step halfway through the attack…as just one of an infinite variety of possible impacts on the MoI (e.g. instantaneous drop, linear drop, logarithmic drop, quadratic drop). At some point-in-time, the attack ends ($t_{\text{attack-end}}$), though there is no guarantee that the organization or its agents are aware of the specific end
time—nor for that matter are they assured of being aware of a specific start time ($t_{\text{attack-start}}$). The chart above depicts a quiescent period after the attack and before ‘recovery’ begins ($t_{\text{recovery}}$), or before the MoI rises above the minimum performance reached as a consequence of the attack. There is no requirement for recovery to start immediately, as the attack may have effects on the MoI that outlast the attack itself. It’s also important to note that there is a space between the minimum performance (MoI$_{\text{min-acceptable}}$) for this MoI and a minimally acceptable threshold set, *a priori*, by one or more leaders of organizations. This threshold may have been set, or may simply be a generalized statement by leadership akin to ‘no performance drop is acceptable!’ This picture does not depict a return to pre-attack levels for this MoI (at $t_{\text{pre-attack reached}}$), indeed there is no universal requirement in all definitions of resilience that this be so, not withstanding Bishop (2011). Indeed, in the happy situation shown above, the forecast is that through adaptation, the attack/attacker makes the organization better in this MoI than they might otherwise have become.

In an attack, however, where the MoI$_{\text{min}}$ drops below MoI$_{\text{min-acceptable}}$, the MoI for the modeled organization would have low resilience, and potentially low-survivability. Such a situation would make recovery all the more daunting as first recovery efforts would be geared to re-gaining the MoI$_{\text{min-acceptable}}$ level of performance.

It’s also feasible that there are indirect measures of resilience for the organization. An example of such could be the cognitive load turbulence due to a contested-cyber environment. During a contested cyber environment, facing degradation, destruction, denial, or disruption of a cyber resource, people will attempt to adapt. Part of their adaptation can be changes to their normal patterns of interaction with other systems and other agents. This change in interaction is an indirect measure of resilience—with very few changes, the effects of the contested cyber environment may be mitigated by the agents. Or the attack could provoke very large changes in interaction patterns. Once the attack has passed, it is unlikely that new interaction patterns recently experienced will *en masse* return to their pre-attack patterns. In this case, we would expect resilience to appear something like the figure below.

The measure of organization (MoO) shown on the vertical axis could, as discussed, be the stability of the cognitive core of activated alters for the decision makers (e.g., the members of the C-Suite). During the attack there is a decrease in stability of those activated cores, and importantly, even after the attack the stability continues to drop. However, after MoO$_{\text{min}}$ is
reached, recovery commences and begins an upward trending but periodic improvement. In the case depicted, the new equilibrium is below the original equilibrium, indicating a permanent effect (MoO_{perm neg effect}) for this attack. If this effect is forecast to be large, a decision maker could use the forecast to potentially make changes in their continuity of operations planning, their rehearsals, or other ways to improve their ability to return to normal operations (MoO_{normal}). We expect to see the periodic nature of improvement prior to equilibrium as a reflection of the echoes of the original change—much as sound waves do not instantly dissipated, the perturbations of organizational adaptation will also not instantly remove themselves from the organization.

Figure 138 Dynamic visualization of resilience for an arbitrary measure of organization (MoO)(Morgan & Lanham, 2012)

Alphabetical Definitions

**Computer Network Attack (CNA)**

“Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy [emphasis added] information resident in computers and computer networks, or the computers and networks themselves.” (Joint Staff J7, 2010a)

**Computer Network Defense (CND)**

“Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities” (CNSS, 2010)
Computer Security (COMPUSEC)

“The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.” (Joint Staff J7, 2010a)

Information Security (INFOSEC)

“The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users.” (Joint Staff J7, 2010a)

Information Assurance (IA)

“Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” (CNSS, 2010; Joint Staff J7, 2010a)

From an operations generalist perspective, IA is a repeatable set of processes that enable informed risk management in the face of uncertainty and competing demands on limited resources.
Appendix 2 Literature Review Bibliometrics

Introduction

This appendix is to document the steps and methodology I used to collect information in support of the Literature Review portion of the dissertation that started on page 10. It is my intention to provide sufficient information and specificity that the reader may duplicate the process I used, and ideally arrive at similar if not identical results. I have made the outputs of the searches into data files and made them available on my personal web page at the following URL: http://www.andrew.cmu.edu/user/mlanham/relatedLit:

Process

The following is a high-level summary of the steps I used to gather and analyze the bibliometric data included earlier in the dissertation.

1. Use Google Scholar to conduct key word, key phrase, collocation, and Boolean-based searches.
2. Use a custom ECMA/JavaScript I wrote, Google Scholar Citation Exporter\(^9\), to mark citations as related to the dissertation. This was a subjective decision based on a number of factors. Those factors included: citation count, title concepts, summary concepts, author(s), and publication.
3. Iterate steps 1 and 2 across each of the query sets I developed.
4. Pre-process collected citations and citation links to reduce duplicates and ensure well formed columns of data. Copy citations’ identifiers and citations’ titles to a separate file for text-based analysis (i.e., Latent Dirichlet Analysis and Latent Semantic Analysis).
5. Import collected citations as Nodes into ORA\(^\text{TM}\)
6. Import collected citation links as Node links into ORA\(^\text{TM}\)
7. Conduct ORA\(^\text{TM}\)-based Analysis

Searches and Search Results

Each of the searches fell into a mental category based on my personal intuition as well as suggestions from fellow students and CASOS faculty. The categories are shown below, with the search strings for each category depicted for future replication. The hyperlinks to the results

\(^9\) This script is an extension, by permission, of Mayank Lahiri’s "Google Scholar™ Citation Exporter." In brief, the original script allows a user to select multiple Google Scholar™ returns and then display the co-citations of those selected results in a new window. The extension resolved fatal errors that accumulated over time as a result of Google changing the HTML used to render the results. The extension then gives the user the option of displaying the results in a comma-limited window with citations at the top, and citation links at the bottom. A user may then cut and paste this displayed information into other files for follow-on processing and analysis.
point to my personal web page on Carnegie Mellon Web Servers. Should, at some future point, CMU remove my personal web page from their servers, I will have moved a copy of that web site to a new locale—Google™ or other search engines should be able to find the site with little difficulty.

Organizational Resilience
1. organizational resilience -child –ecology Output: pdf
3. organizational adaptation to (crisis OR attack OR degraded) –animal Output: pdf

Cyber Command and Control
4. (resilient OR adaptive) (centralized OR decentralized) command and control cyber environments - "natural resource" Output: pdf
5. military cyber (“command AND control” OR C2) degraded AROUND(3) environments Output: pdf

Cyber Security
6. cyber vulnerability military (“command AND control” OR C2) (measure OR assess) Output: pdf
7. cyber sociotechnical organization vulnerability -scada –power Output: pdf
8. military effects of cyber attacks US OR Korea OR Estonia OR Georgia OR Lithuania Output: pdf
9. cyber military “mission assurance” Output: pdf
10. (perceived OR perception) and (reliance OR reliant) and ("information technology" OR cyber) –teaching –patient –medicine –entertainment Output: pdf

Modeling and Simulation
11. agent based modeling simulation organizational resilience "information technology" -water –agriculture –genetic Output: pdf
12. "discrete event" (modeling OR simulation) organizational resilience "information technology" -water –agriculture –genetic Output: pdf
13. "system dynamics" (modeling or simulation) organizational resilience "information technology" -water –agriculture Output: pdf
14. "business process" (modeling or simulation) organizational resilience "information technology" -water –agriculture Output: pdf
15. model organization reaction to loss of IT Output: pdf

SNA and Resilience to Cyber Vulnerability
16. organization AROUND(5) modeling and simulation "text mining" topic –gene Output: pdf
17. sociotechnical system vulnerability modeling (cyber or "information technology") Output: pdf
HRO and Resilience to Cyber Vulnerability

22. (“High Reliability Organization” OR HRO) resilience Output: pdf
23. “Resilience Engineering”

Pre-processing Collected Data

This step principally involved the merging of the multiple takes from the queries depicted in the Searches and Search Results section, removing duplicates, and ensuring well-formed data in each column of the merged data files. For cells with entries clearly placed one or two cells left or right of where they should be, I simply moved them to their correct position. For cells with no data, or partial data, I left them as was and conducted additional merging and cleaning within ORA™.

The data files end up in two (2) distinct comma separated variable (CSV) files: one with the citations’ information (relatedLit_Citations.csv, URL: http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Citations.csv) and one with the links between citations (relatedLit_Links.csv), URL http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Links.csv.

Importing Collected Data into ORA™

Metanetwork Creation and Preparation

1. Created a new, empty, metanetwork, which I called Dissertation Related Literature

Created the following node sets, with 1 node per node set as a place holder

1.1. Author (as ORA™ type Agent)
1.2. Article (as ORA™ type Resource)
1.3. Journal (as ORA™ type Organization)
1.4. Publisher (as ORA™ type Organization)
1.5. Year (as ORA™ type Event)

Created the following networks to link the node sets, though they are all empty

1.6. Article x Article
1.7. Author x Article
1.8. Journal x Article
1.9. Publisher x Journal
1.10. Year x Article

Import Node Sets and Networks

**Article Node Set (IDs only) and Article x Article Network**

To import the citation node identifiers, as well as import the links between the identifiers, I imported the `relatedLit_Citations.csv` first and had ORA™ create nodes in the Article node set for each unique ID it processed.

1. Within ORA™, selected the Article x Article

2. Selected from the menu, File ➔ Data Import Wizard...

   2.1. Selected the option labeled Import Excel or text delimited files
   2.2. Selected the option labeled Table of network links
   2.3. Selected the button labeled Next
   2.4. Selected the option labeled Add to the existing metanetwork: and ensured I selected Dissertation Related Literature
   2.5. Selected the button labeled Next
   2.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the `relatedLit_Links.csv` file
   2.7. In the Step 2 portion of the UI
      2.7.1. Selected CITEDBY and CITED
      2.7.2. Set the type in each column to Resource
   2.8. In the Step 3 portion of the UI
      2.8.1. Selected the button labeled New to define a new network of links
      2.8.2. Selected citedBy in the Source Node Name column
      2.8.3. Selected cited in the Target Node Name column
      2.8.4. Selected link in the Link Value column
      2.8.5. Typed Article x Article in the Network Name column
      2.8.6. Placed a check mark in the Create new nodes for unrecognized node names
   2.9. Selected the button labeled Finish
   2.10. Selected from the menu, File ➔ Save

For readers interested in performing the steps from 2.6 to 2.8 using a saved configuration file, save the source code listed under the subheading Article x Article within the section entitled **Error! Reference source not found.** to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from 2.6 to 2.8.
Article Nodes’ Attributes

Next I finished the importation of all the citations’ attributes and information stored in the relatedLit_Citations.csv file.

1. Selected the Article node set
3. Selected from the menu, File→Data Import Wizard...
   3.1. Selected the option labeled Import Excel or text delimited files
   3.2. Selected the option labeled Table of node attributes
   3.3. Selected the button labeled Next
   3.4. Selected the metanetwork to modify by placing a check mark in the box next to the Dissertation Related Literature metanetwork name.
   3.5. Selected Next
3.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the relatedLit_Citations.csv file
3.7. In the Step 2 portion of the UI, I selected citationId in the drop down box for Use this column for node names
3.8. In the Step 3 portion of the UI
   3.8.1. For the citationUrl column, changed the type to URI
   3.8.2. For the citedByUrl column, changed the type to URI
   3.8.3. For the relatedArticlesUrl column, changed the type to URI
   3.8.4. For the clusteredArticles column, changed the type to URI
   3.8.5. For the clusteredArticles column, changed the type to URI
   3.8.6. For the title column, changed the type text
   3.8.7. For the citedByCount column, changed the type Number
   3.8.8. De-selected journal column
   3.8.9. De-selected publisher column
   3.8.10. De-selected year column
   3.8.11. De-selected author0 to author5 columns
   3.8.12. De-selected link column
   3.8.13. Selected Create new nodes for unrecognized node names. This selection will support the creation of nodes that were not in the links file, that are otherwise isolates in the citation metanetwork.
3.9. In the Step 4 portion of the UI
   3.9.1. Selected the button labeled Clear All
   3.9.2. Selected the Article nodeset
3.10. Selected the button labeled Finish
3.11. Selected the button labeled OK in the window that popped up reporting the import status.
3.12. Selected from the menu, File→Save

There is no saved configuration file for this step like where was for importing a network.
Author x Article Network

4. Selected the Author x Article

5. Selected from the menu, File → Data Import Wizard...

5.1. Selected the option labeled Import Excel or text delimited files
5.2. Selected the option labeled Table of network links
5.3. Selected the button labeled Next
5.4. Selected the option labeled Add to the existing metanetwork: and ensured
   I selected Dissertation Related Literature
5.5. Selected the button labeled Next
5.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had
   stored the relatedLit_Citations.csv file
5.7. In the Step 2 portion of the UI
   5.7.1. Selected CITATIONID, set the Class to Resource, and the Name to Article
   5.7.2. For AUTHOR0 to AUTHOR4, select the column
          5.7.2.1. Set the Class to Agent
          5.7.2.2. Set Name to Author
5.8. In the Step 3 portion of the UI
   5.8.1. Selected the button labeled New to define a new network of links
   5.8.2. Selected author0 in the Source Node Name column
   5.8.3. Selected citationID in the Target Node Name column
   5.8.4. Selected link in the Link Value column
   5.8.5. Typed Author x Article in the Network Name column
   5.8.6. Repeat steps 5.8.1 to 5.8.5 for Author1 to Author4
   5.8.7. Placed a check mark in the Create new nodes for unrecognized node names
5.9. Selected the button labeled Finish
5.10. Selected from the menu, File → Save

For readers interested in performing the steps from 2.6 to 2.8 using a saved configuration file, save the source code listed under the subheading Author x Article within the section entitled Error! Reference source not found. to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from 2.6 to 2.8.

Journal x Article Network

6. Selected the Author x Article

7. Selected from the menu, File → Data Import Wizard...

7.1. Selected the option labeled Import Excel or text delimited files
7.2. Selected the option labeled Table of network links
7.3. Selected the button labeled Next
7.4. Selected the option labeled Add to the existing metanetwork: and ensured I selected Dissertation Related Literature
7.5. Selected the button labeled Next
7.6. To the right of the Step 1 dialog box, I selected Browse and navigated to where I had stored the relatedLit_Citations.csv file
7.7. In the Step 2 portion of the UI
   7.7.1. Selected CITATIONID, set the Class to Resource, and the Name to Article
   7.7.2. Selected Journal, set the Class to Organization, and the Name to Journal
7.8. In the Step 3 portion of the UI
   7.8.1. Selected the button labeled New to define a new network of links
   7.8.2. Selected journal in the Source Node Name column
   7.8.3. Selected citationID in the Target Node Name column
   7.8.4. Selected link in the Link Value column
   7.8.5. Typed Journal x Article in the Network Name column
   7.8.6. Placed a check mark in the Create new nodes for unrecognized node names
7.9. Selected the button labeled Finish
7.10. Selected from the menu, File→Save

For readers interested in performing the steps from 2.6 to 2.8 using a saved configuration file, save the source code listed under the subheading Journal x Article within the section entitled Error! Reference source not found. to an XML file. Select that file using the Load configuration file button to automatically perform (or repeatedly perform) steps from 2.6 to 2.8.

Publisher x Journal Network

I repeated the steps used to create the Journal x Article network making the appropriate substitutions for network and file names.

Year x Article Network

I repeated the steps used to create the Journal x Article network making the appropriate substitutions for network and file names.

Concept Nodeset, Text Nodeset and Semantic Network

1. Copied the Citation’s Node Name and Node Title columns to a tab-delimited text file. The Node Name column contains the Google Scholar™ identifier for the citation, and the Node Title column contains the citation’s title text as presented by Google Scholar™.
2. Used a small Java application, CitationSplitter.java, (URL: http://www.andrew.cmu.edu/user/mlanham/code/CitationSplitter.java) to convert this text file into a directory containing a file per row in the text file. Each file uses the Node Name
3. Used AutoMap’s Data-To-Model (D2M) (Kathleen M. Carley, Bigrigg, et al., 2011; Lanham et al., 2014; Lanham, Morgan, Carley, et al., 2011) process to ingest this directory of citation titles to create a concept list. The D2M wizard user interface (UI) is shown in Figure 139. The concept list is a list of distinct words in the corpus of citation titles.

3.1. I used a standard thesaurus available to CASOS researchers as well as a thesaurus I personally constructed over the course of multiple iterations of data reduction and cleaning. The personal AutoMap thesaurus is available the following URL http://www.andrew.cmu.edu/user/mlanham/relatedLit/relatedLit_Thesaurus.csv. I have no objections to future readers incorporating this thesaurus into their work so long as they cite this dissertation within the relevant work.

After creation of the concept list, I ‘cleaned’ the concept list in support of creating semantic co-location networks of concepts in the corpus. The D2M-process, in addition to the concepts, provides the term-frequency inverse document frequency (TFIDF) as calculated using Equation 47 through Equation 49 (Kathleen M. Carley, Columbus, et al., 2011). The initial cleaning used the distribution of the TFIDF values depicted in Figure 140 to establish a cut-off of $4.19 \times 10^{-4}$. This equates to including, in the first pass of cleaning, 90.442% of the concepts when sorted from largest to smallest TFIDF values, depicted in Figure 141. The descriptive statistics for this pass are shown in Table 60.

$$term_x \text{ frequency (tf)} = \frac{\text{Count of } term_x}{\text{Number of terms in document}_y} \quad (50)$$

Equation 47 Term Frequency for Concept $x$
inverse document frequency (\( idf \)) = \( \log\left(\frac{\text{number of documents in corpus}}{\text{number of documents with } \text{term}_x}\right) \) \hspace{1cm} (51)

Equation 48 Inverse Document Frequency for Term x in Corpus

\[ \text{TF-IDF} = tf \times \text{idf} \] \hspace{1cm} (52)

Equation 49 Term Frequency x Inverse Document Frequency (TFIDF)

Table 60: Descriptive Statistics for D2M of Citation Titles

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Concepts, Pre-Cleaning</td>
<td>6,591</td>
<td>Number of Concepts, Post-Cleaning</td>
<td>4,276</td>
</tr>
<tr>
<td>TFIDF Mean</td>
<td>0.00088</td>
<td>TFIDF Standard Deviation</td>
<td>0.00187</td>
</tr>
<tr>
<td>TFIDF Median</td>
<td>0.00032</td>
<td>TFIDF Skew</td>
<td>6.59235</td>
</tr>
<tr>
<td>TFIDF Mode</td>
<td>0.00012</td>
<td>TFIDF Kertosis</td>
<td>63.0528</td>
</tr>
<tr>
<td>TFIDF Trend Equation(^{10})</td>
<td>( y = 2.3563x^{-1.122} )</td>
<td>R(^2) for Trend Equation</td>
<td>0.9174</td>
</tr>
<tr>
<td>TFIDF Quartiles(^{11}) (75%, 50%, 25%)</td>
<td>0.00617</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.00237</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0.000849</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 140 Concept\(^{12}\) x TFIDF\(^{13}\)

\(^{10}\) Using Excel for Mac 2010, ‘Trend line’ functionality built into Excel’s Charting Functions

\(^{11}\) TFIDF values sorted in descending order, cumulatively summed until 25\%, 50\%, and 75\% of the area under the curve is reached. 50\% percent deviates from median as some TFIDF values repeat—many concepts have the same TFIDF values

\(^{12}\) Concepts not depicted in graph for visual clarity of the graph

\(^{13}\) TFIDF values sorted in descending order
3.2. The second pass of cleaning involved deleting concepts with a frequency of one (1) and then using ORA™ to remove isolates created from the previous steps.

**Cleaned Article node set**
1. Deleted articles with non-English titles
2. Transformed networks to delete isolates based on entire metanetwork and saved as new file

**Cleaned Author node set**
1. Removed Asian script names
2. Used ORA™’s clean menu button to remove duplicates
3. Used ORA™’s Clean menu button to look for names 1 character edit-distance from others: An example would be M Lanham and MJ Lanham. Disambiguated with aid of scholar.google.com and google.com, ORA™ visualization, and ORA™ metrics. Merger if confident of names referring to the same individuals.
4. Used ORA™ Key Entity Report to look for any entries in top 50 that were visually similar. Used similarity to focus addition search for duplicates. Merged as necessary.
5. Transformed networks to delete isolates based on entire metanetwork and saved as new file

**Cleaned Concept node set**
1. Deleted concepts with UTF-8 symbols that were not rendered as meaningful text
2. Merged a number of nodes that were generalizations of each other
3. Ran Hot Topics Report on Semantic Network and had ORA™ depict the top 50 entries. The report depicted no entries that were generalizations of each other

**Manipulate Networks**

**Co-Authors**
1. Transposed Author x Article
2. Multiplied Author x Article with transpose to get co-authors

**Articles per Year**
1. Transposed Year x Article

---

14 TFIDF values sorted in descending order
2. Multiplied Author x Article with transpose above to get articles per year

Move .edu organizations from Publisher to new nodeset School of type Organization

3. Selected *.edu and moved them to a new nodeset
4. Merged schools of same 2\textsuperscript{nd} level domain unless I was aware of a 3\textsuperscript{rd} level domain being a specific research lab/center

Move [BOOK] and [B] articles to new nodeset called Book of type Resource

5. Selected [BOOK|B] articles and moved them to a new nodeset

Move [C] articles to new nodeset called Citation of type Resource

6. Selected [C] articles and moved them to a new nodeset

Data-to-Model AutoMap ScriptRunner file

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<Script>
  <Utilities>
    <Procedures>
      <DataToModel attributes="" numThreads="3"
projectDirectory="V:\dissertation\ora\relatedLit\automap_outputs"
standardThesaurus="**a unique to CASOS thesaurus**"
textDirectory="V:\dissertation\ora\relatedLit\inputs\IDs_and_Titles_Split"
userThesaurus="V:\dissertation\ora\relatedLit\inputs\relatedLit_Thesaurus.csv"/>
    </Procedures>
    <CEMap/>
    <Extractors/>
    <PreProcessing/>
    <Generate/>
    <PostProcessing/>
  </Utilities>
  <Settings>
    <AutoMap deleteTemp="n" intermediate="y"
tempWorkspace="C:\temp\am3temp" textDirection="LT"
textDirectory="V:\dissertation\ora\relatedLit\inputs\IDs_and_Titles_Split"
textEncoding="UTF-8"/>
  </Settings>
</Script>
```

Article x Article

```xml
<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
  <metaMatrix id="Meta Network">
    <create>
      <nodeset type="Resource" id="Article" />
      <nodeset type="Resource" id="Article" />
      <graph sourceNodesetId="Article" targetNodesetId="Article" id="Article x Article" />
    </create>
  </metaMatrix>
</queryScript>
```
Author x Article

<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
<metaMatrix id="Meta Network">
<create>
<nodeset type="Resource" id="Article" />
<nodeset type="Agent" id="Author" />
<nodeset type="Agent" id="Author" />
<nodeset type="Agent" id="Author" />
<nodeset type="Agent" id="Author" />
<nodeset type="Agent" id="Author" />
<graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x Article" />
<graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x Article" />
<graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x Article" />
<graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x Article" />
<graph sourceNodesetId="Author" targetNodesetId="Article" id="Author x Article" />
</create>
<query>
<input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
<output>
<graph id="Author x Article">
<fromColumn index="10" makeUnique="false" />
<toColumn index="0" makeUnique="false" />
<weightColumn index="15" makeUnique="false" />
</graph>
<graph id="Author x Article">
<fromColumn index="11" makeUnique="false" />
<toColumn index="0" makeUnique="false" />
<weightColumn index="15" makeUnique="false" />
</graph>
<graph id="Author x Article">
<fromColumn index="12" makeUnique="false" />
<toColumn index="0" makeUnique="false" />
<weightColumn index="15" makeUnique="false" />
</graph>
<graph id="Author x Article">
<fromColumn index="13" makeUnique="false" />
<toColumn index="0" makeUnique="false" />
</graph>
</query>
</metaMatrix>
</queryScript>
Journal x Article

<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
<metaMatrix id="Meta Network">
<create>
<nodeset type="Resource" id="Article" />
<nodeset type="Organization" id="Journal" />
<graph sourceNodesetId="Journal" targetNodesetId="Article" id="Journal x Article" />
</create>
<query>
<input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
<output>
<graph id="Journal x Article">
<fromColumn index="7" makeUnique="false" />
<toColumn index="0" makeUnique="false" />
<weightColumn index="15" makeUnique="false" />
</graph>
</output>
</query>
</metaMatrix>
</queryScript>

Publisher x Journal

<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
<metaMatrix id="Meta Network">
<create>
<nodeset type="Organization" id="Journal" />
<nodeset type="Organization" id="Publisher" />
<graph sourceNodesetId="Publisher" targetNodesetId="Journal" id="Publisher x Journal" />
</create>
<query>
<input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
<output>
<graph id="Publisher x Journal">
<fromColumn index="8" makeUnique="false" />
<toColumn index="7" makeUnique="false" />
<weightColumn index="15" makeUnique="false" />
</graph>
</output>
</query>
</metaMatrix>
</queryScript>
Year x Article

<?xml version="1.0" encoding="UTF-8"?>
<queryScript>
<metaMatrix id="Meta Network">
  <create>
    <nodeset type="Resource" id="Article" />
    <nodeset type="Event" id="Year" />
    <graph sourceNodesetId="Year" targetNodesetId="Article" id="Year x Article" />
  </create>
  <query>
    <input>V:\dissertation\ora\relatedLit\relatedLit_Citations.csv</input>
    <output>
      <graph id="Year x Article">
        <fromColumn index="9" makeUnique="false" />
        <toColumn index="0" makeUnique="false" />
        <weightColumn index="15" makeUnique="false" />
      </graph>
    </output>
  </query>
</metaMatrix>
</queryScript>
Appendix 3 Data to Model Implementation Details

Introduction

This appendix is to document the steps and methodology I used to collect and process information in support of rapidly developing the sociotechnical models of Strategic, Operational and Tactical set of US Department of Defense (DoD) commands. This material expands upon and extends the work briefly discussed in the Data and Models chapter of the dissertation that started on page 69. It is my intention to provide sufficient information and specificity that the reader may duplicate the process I used for each of the three (3) D2M generated models, and ideally arrive at similar if not identical results. I have made the Adobe Acrobat™ files (.pdf) available on my personal web pages at in three (3) zip files: strategic.zip, operational.zip, and tactical.zip at the following URL: http://www.andrew.cmu.edu/user/mlanham/data2model. I have also made the DoD-specific thesaurus, in what CASOS refers to as Master Thesaurus format, available as well as the model-specific thesauri. It is my intention that, for organizations who decide to use the D2M-process, these thesauri be available and useful. Additionally, as an employee of the USG, the work I have done while pursuing this research should be available to the public.

Retrieving input corpus

The bash shell script shown below retrieves the set of PDF documents for each model of interest in the dissertation. There were some documents that, though within the list of documents in later sections, I had to manually download as the organizations that host the documents have placed them behind authentication schemes that wget does not support.

Bash script for retrieval, text extraction, and text file splitting

The bash script is hosted on my personal web page at http://www.andrew.cmu.edu/user/mlanham/data2model/get_sets_as_text.sh and the algorithm for the script is below.

For each model in model list
  Create pdf directory, if needed
  Use wget to retrieve all entries in corpus_list.txt
  For each pdf file, use pdftotext to extract file_name.txt
  Create split_texts dir, if needed
  Move extracted text files to split_texts dir
  For each extracted text file, split it into 64KB chunks using split
List of documents for strategic level corpus and the URLs to retrieve them
42. http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf
List of documents for operational level corpus and the URLs to retrieve them

1. Air Force Instruction (AFI) 13-1AOCV3.pdf
2. Air Force Tactics Techniques and Procedures (AFTTP) 3-3.2 AOCNov07.pdf
Corpus augmentation

Augmenting corpus—figures to text

Figures within texts remain indecipherable to the `pdftotext` application as well as the AutoMap program. As such, the author and a collaborator, Jon Licht, translated select figures from AFTTP 13-3.2 to text for ingest by AutoMap and for use in previous work. Those figures were:

<table>
<thead>
<tr>
<th>Figures</th>
<th>1.1</th>
<th>1.2</th>
<th>1.3</th>
<th>3.1</th>
<th>3.2</th>
<th>3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numbers</td>
<td>3.4</td>
<td>3.5</td>
<td>3.6</td>
<td>3.7</td>
<td>4.1</td>
<td>4.2</td>
</tr>
</tbody>
</table>

Though undoubtedly the generated models could benefit from translating other figures to text, there is at present insufficient evidence to assess the improvement. Many of the cross functional groups’ relationships and membership depicted in AOC structural diagrams were not in the sets as text—thus substantiating the possible usefulness of figure-to-text translation. However, as discussed in the Data and Models chapter starting on page 69, it remains an open question if such effort will always work, will, with statistical significance, appropriately update models, or if, in the absence of statistical significance, provide qualitative improvements to the models.

Additionally, translating pictures into their respective “one thousand words” is a label intensive process that is clearly not aligned with the key word ‘Rapid’ in the title of the dissertation. Though figures and pictures remain relevant and useful to a large set of the human readers of doctrine, it is doubtful that they will provide meaningful assistance.

Retrieving input corpus

Augmenting corpus—coercing links via AutoMap

ORA™ does not yet have the ability to capture a change list, a set of changes created by the user, for edges between nodes within the ORA™ UI. One way I captured additions of
links between existing nodes was through the use of a manually created and updated Isolate Correction text file. This file, in pseudo-English, supports the automated creation of links between multiple node types using either the reduced form name of a node (e.g., i_t) or other forms that the thesaurus is ready to process correctly (e.g., information technology). Through the deliberate creation of sentences with words that should be linked to create an accurate model, AutoMap can be manipulated into creating links a researcher would otherwise have to create by hand. In this way, a modeler can reduce deficiencies in the model AutoMap generates from the corpus of text.

This technique, like the figures-to-text translation discussed above, has its drawbacks. It is easy, and sometimes entirely appropriate to hand-link dozens to hundreds of nodes to other nodes—even if not readily repeatable by other researchers attempting to replicate and extend work. It is also easy, sometimes appropriate to type the relationships in sentences knowing the names of the nodes and the word(s) that capture the relationship link between the nodes. This process has the advantage of being repeatable for future researchers, as well as slowly building up a repository of relationships explicitly drawn in figures, but frequently not addressed as text. The final draw back for this technique is the labor drain to author the links-as-sentences file. Such labor drain runs contrary to the rapid initial model creation implied in the dissertation model. It may however be suitable for model sustainment and refinement over time.

Pre-processing DoD corpus

Over the course of the dissertation, there were several opportunities to refine the process and reduce the amount of thesaurus refinement and ORATM-based model refinement. This section addresses each of those opportunities and the techniques I used to conduct pre-processing of the corpus before using AutoMap.

Regular expression deletion of noise patterns

Many of the documents in the corpus have headers or footers that contain verbiage that, if retained in the final models, would unduly weight the repeated concepts. There are also other word patterns that AutoMap, as of 2013, is incapable of removing or adequately addressing. To resolve this situation, I used bash shell code below to invoke perl and pre-process the corpus to replace the identified patterns with empty white space. Having a script
available and functioning reduces the development time for future researchers and / or organizations desirous of using this dissertation’s process. The overhead in terms of processing time was minimal, on the order of a few minutes per corpus.

```
#!/usr/bin/sh
#
#3rd pattern catches Doc Origination +
# number [.number[alpha][.-][number]]
#4th pattern catches Title + number, USC, Section +
# Number Doc Original + number, doc-title
#5th pattern cleans up multiple underscores to
# single underscore
#6th pattern drops trailing underscores from words
#7th pattern drops leading underscores from words
#8th pattern drops patterns of junk chars created(?)
# during pdf-to-txt conversion
perl -0744pi -e \'
's/Department of Defense Instruction \((DODI)\) /DODI/g;
 s/Joint Publication\Joint Publication\w*\JP\)/JP/g;
 s/(EO|HSPD|PDD|CJCSI|NSPD|DO[DI]\JP\AR|AFDD|FM|TC|DIAM
 |CJCSN|CJCSM|AFTTP|DCID|AFDDs|j_p|DODDs|APP|STANAG|TM]\[ -.]?([0-9]+)(?:[.-]([0-9]*))?([A-Z]*)(?:[.-]([0-
9]+))?([:-.])([A-
Z]+))?,(([^\r\n.]*\r[^\r\n\.,]*)){0,2})[.,]?/lc($1)."$_2_ $3_.$4_$5"/gie;
 s/(Title) ([0-9]+)\ (?, USC\ ?, (?:Section ([0-
9]+))?([^\r\n.]*\r[^\r\n\.,]*))?/lc($1)."$_2_$4"/gie;
 s/_+/_/g;
 s/\b_//g;
 s/_\b//g;
 s/^Table.*\[0-9]+$/g;
 s/^Figure\.*\[0-9]+$/g;
 s/[ÔøÔΩ'Ä¢≈√欩\?]*/g;' $1
```

Case sensitive application of DoD and model-specific thesaurus

Since the DoD makes extensive use of acronyms, I needed to have a case sensitive way of disambiguating all-capital-letter acronyms from words that might otherwise be in the thesaurus. To conduct the disambiguation, I applied the DoD thesaurus in a case sensitive manner, using a short Python script whose pseudo-code is below—the actual python script is on my personal web page at

http://www.andrew.cmu.edu/user/mlanham/code/applyAcronymThesaurus.py.
The Python script performs word-level, case sensitive, regular expression matching as well as attempting to match words surrounded by parenthesis. The DoD uses a writing style where authors spell out an acronym then specify the acronym in parenthesis (e.g., Listening Post (LP)). The script also performs a function that AutoMap developers have sense incorporated—turning hyphenated words into ngrams as a first-pass heuristic for ngram identification.

read thesaurus into Python key-value dictionary
for each text file
  for each line of text
    for each word in line
      if word in thesaurus
        if meta-ontology column == #delete
          delete word in line
        else replace word in line with
          thesaurus word
      else if word minus 1 char in thesaurus
        if meta-ontology column == #delete
          delete word in line
        else replace word in line with
          thesaurus word
      if word contains hyphen
        convert word to ngram
flush read/writer buffers periodically

Metanetwork encoding heuristics for thesaurus refinement

The thesaurus refinement process is rife with opportunities for inconsistencies. Though follow-on researchers may choose to disagree with the encoding choices I have made, the table below depicts the heuristics I used when assigning concepts of interest to one of the ontological categories in the metanetwork framework.

<table>
<thead>
<tr>
<th>Key word/words in original text segment</th>
<th>Metanetwork ontology category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most words with –ly,-est suffixes</td>
<td>Attribute</td>
</tr>
<tr>
<td>(based on generalization that the words with those endings are adverbs)</td>
<td></td>
</tr>
<tr>
<td>Most words with –ed suffix</td>
<td>Knowledge</td>
</tr>
<tr>
<td>(based on generalization that the past-tense of a verb implies knowledge of the execution of that verb)</td>
<td></td>
</tr>
<tr>
<td>Ranks (SES, GS, E1-E9, O1-O10)</td>
<td>Attribute</td>
</tr>
<tr>
<td>Request, Responsibilities, Duties</td>
<td>Task</td>
</tr>
<tr>
<td>Chief, commander, director, system, processor, tool, database</td>
<td>Agent</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Specific named people relevant to project, Specific named position within orgs filled by exactly one person (e.g. Commander, Director, Secretary)</td>
<td></td>
</tr>
<tr>
<td>Authority (Ability to grant/deny permission)</td>
<td>Resource</td>
</tr>
<tr>
<td>Critical</td>
<td>Belief</td>
</tr>
<tr>
<td>Conference</td>
<td>Event</td>
</tr>
<tr>
<td>Shared information, if when given to another, the originator still has the information (e.g., lists, opords, plans, oplans, procedures)</td>
<td>Knowledge</td>
</tr>
<tr>
<td>Area, Facility, installation, base, operations area, post, camp, station</td>
<td>Location</td>
</tr>
<tr>
<td>Program</td>
<td>Task (e.g. WMD Counter-proliferation), sometimes organization when I can tie the lone word into a N-Gram for disambiguation</td>
</tr>
<tr>
<td>Agency, branch, brigade, center, committee, company, council, detachment, division, fleet, MEU, MEB, Mission, office for *, office of *, organization, platoon, program office, <em>service</em>, named units/organization/ship, squadron, team, united, wing, ship(s), S1-S9, G1-G9, same for A/N/M/J-staff codes</td>
<td>Organization (specific ships, when discussed as a resource [e.g. USS JFK was decommissioned/overhauled) get coded as “resource” instead of org)</td>
</tr>
<tr>
<td>Specific/named (e.g. fighter wing, division, brigade, agency) collection of people or organizations (by composition or aggregation), * force(s), alliance</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Budget</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Generic/unnamed (e.g. fighter wing, division, brigade, agency) collection of people or organizations (by composition or aggregation), * force(s), alliance</td>
<td><em>Support</em></td>
</tr>
<tr>
<td>Causeway, equipment, radios, antenna, fuel, medal, missile, package, * Program (e.g. Contingency Program, DITSCAP, DIACAP), tanks, trucks, airplanes, programme</td>
<td>a generalized service provided (often) by one party to another party</td>
</tr>
<tr>
<td>An instance of a physical asset, if when given to another, the originator no longer has it AND the asset is not frequently synonymous with an ‘organization’</td>
<td></td>
</tr>
<tr>
<td>A computer system component (e.g. DVD ROM drive, keyboard) Computer protocol(s), radio frequency(ies), subsystem(s),</td>
<td></td>
</tr>
<tr>
<td><em>Support</em></td>
<td></td>
</tr>
<tr>
<td>Named computer systems, named information technology, named satcom systems, named</td>
<td>Agent (with Agent Type attribute==it_system) – if it passes knowledge/information between other agents/organizations. Using computers imposes a cognitive load on people as well. Finally, intention is to model within construct the following: p(forgetting)&gt;0 &amp; &lt;&lt; 1; p(! interact) &gt;0 &amp; &lt;&lt; 1; p(tx err)&gt;0 &amp; &lt;&lt; 1.</td>
</tr>
</tbody>
</table>
Using frequency as culling decision input variable

At least for some measures, the heuristic of deleting nodes with low ‘frequency’ attributes will sabotage the use of the measure. Likewise the deleting of pendants, recursively or not, may inflict unexpected changes to the network.

The D2M process, when generating the metanetwork, will generate several attributes per node in each of the node classes. One of those attributes is ‘Frequency,’ which is a simple count of how many times the concept (or its mapped-from predecessor) has appeared in the sets. This attribute does not, in isolation, provide a modeler with high confidence that the node(s) is worthy of deleting. I certainly ran across a number of instances when building these three models where the ‘frequency’ of a node was an order of magnitude lower than top
nodes, yet other network measures revealed the node was relevant to the model for its position in the network structure as well as serving as a conduit from one node class to another.

In the specific case of the proposed static resilience measure, the measure requires the counting of near-isolated nodes in three node sets: agents; resources; and tasks. With the intuition that too many nearly isolated nodes leads to too many points of degraded access to people, resources, and tasks, it should be apparent to the reader that removing pendants necessarily decreases the number of nearly-isolated nodes. This is especially true for recursive deletion of pendant chains—where a chain of nodes is connected to nothing other than the next element of the chain.
Appendix 4 Virtual Experiment How-To Guide

This appendix repeats information from a research project that preceded the dissertation discussed elsewhere in this work. However, the methodology and practical how-to guide should benefit future researchers as well as those desiring to critique my work. This appendix describes exactly how the supporting infrastructure and the actual virtual experiments were carried out at a re-execution level of detail.

**SVN or other Shared-work Repository**

I’ve been using SVN as the code repository for all my work. I will write this recipe as if the reader will likewise be using SVN. I leave modifications and changes of the recipe to the reader if they using Git, CVS, SourceSafe, or some other technology/capability.

**Create a named repository**

I usually ask the SVN repository administrator to create a repository using some shortened version of the project name—if feasible. For example, if the project name is “Learned Multi-Level Resilience,” I ask for a repository project called *multi-level*.

**Checkout the named repository**

Of course, a SVN client can checkout a project to a directory using the project’s name or some arbitrary name. The choice is user specific and should be irrelevant to the remainder of this recipe.

**Create a Directory Structure**

Within the (presumably brand new and empty) project directory, create a directory structure. This structure is inherently specific to the researcher or the team of researchers. If a team, defining and settling on it early, though allowing modifications later, will make collaboration easier.

I have created several directory trees and depict them below starting at the project directory entitled *multi-level*. For the dissertation work, I replaced “multi-level” with “dissertation.”
The two folders of immediate interest to the virtual experiment researcher are the *scriptsAndApps* folder and the *construct* folder. As depicted in Figure 142, there are several sub-folders in the *scriptsAndApps* folder.

**Figure 142 Directory structure for virtual experiments**

Within the *construct* folder there are two folders, both required for the proper functioning of the automated scripts created for the learned multi-level resiliency project. The folders have the names *inputDecks* and *runs*. This tree is below in Figure 143.

**Figure 143 Directory structure for construct within virtual experiment directory structure**

*CondorPreparation* - This folder is for the scripts and applications. Those scripts and applications pre-process inputs and write temporary outputs to disk. The folder also holds some helper scripts and .jar files used by the individual condor clients to help the researcher identify
problematic machines in the condor cluster. The .jar file is from the directory tree rooted in the javaUtils folder which is the root of an Eclipse IDE project.

*NetworkGenerator* - This folder is for the Java-based application to take the temporary outputs from the preparation scripts, generate construct networks, and write them to disk. It is the root of an Eclipse IDE project. The resultant exported executable jar is copied to a location I will discuss shortly.

*CondorPostProcess* - This folder holds several shell scripts (bash and perl) that help the researcher identify problems with the output from a condor run.

*runDataAggregator* - This folder is for the Java-based application to take the outputs of a construct run, conduct data reduction and processing enroute to information. It is the root of an Eclipse IDE project.

**Input Files**

The construct input deck can refer to one or more external files for loaded a simulation. The deck for the Multi-Level Project refers to a params.csv file that lists a number of key-value pairs. The reader will note params.csv does not exist, in the inputDecks folder. The preprocessing scripts automatically generate the params.csv from the params_template.xls file.

The params_template.xls file serves several functions

- It supports a single point of entry for variables (thereby reducing the probability of mistyping parameters and/or their values elsewhere)
- It supports rapid and automatic generation of XML needed to define <var> elements in the input deck. The Researcher may still need to copy the XML to the input deck manually.
- It supports rapid and nearly automatic generation of XML relevant to defining <networks> or <operations> elements in the input deck. The Researcher may still need to copy the XML to the input deck manually.
- It supports the rapid and automatic generation of params.csv files unique to each configuration of the virtual experiment as well as the directory structure needed to isolate each of those configurations from the others.
- It supports the rapid and automatic data reduction, aggregation, and output of meaningful results by using the single point of entry for key-value pairs
Params_template.xls

This file, as of April 2013, needs to remain in the pre-Excel 2007 format of .xls.

*Warning: Do not use the .xlsx format, as the perl script processing the file uses a CPAN module that does not support the .xlsx format.*

The contents of params_template.xls are worth reviewing, column by column.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Line</td>
<td>value</td>
<td>type</td>
<td>src</td>
<td>tgt</td>
<td>linktype</td>
<td>vars</td>
</tr>
<tr>
<td>2</td>
<td>0 &amp;attack_email_prob</td>
<td>0</td>
<td>float</td>
<td></td>
<td></td>
<td></td>
<td>value=&quot;ReadFromCSVFile[params.csv,0,constructType=param_val_file,col=param_val_csv]&quot;/</td>
</tr>
<tr>
<td>3</td>
<td>1 &amp;attack_fdf_prob</td>
<td>0</td>
<td>float</td>
<td></td>
<td></td>
<td></td>
<td>&lt;var name=&quot;&amp;attack_fdf_prob&quot; value=&quot;ReadFromCSVFile[params.csv,1,constructType=param_val_file,col=param_val_csv]&quot;/&gt;</td>
</tr>
<tr>
<td>4</td>
<td>2 &amp;attack_phone_prob</td>
<td>0</td>
<td>float</td>
<td></td>
<td></td>
<td></td>
<td>&lt;var name=&quot;&amp;attack_phone_prob&quot; value=&quot;ReadFromCSVFile[params.csv,2,constructType=param_val_file,col=param_val_csv]&quot;/&gt;</td>
</tr>
<tr>
<td>5</td>
<td>3 &amp;attack_prob</td>
<td>0</td>
<td>float</td>
<td></td>
<td></td>
<td></td>
<td>&lt;var name=&quot;&amp;attack_prob&quot; value=&quot;ReadFromCSVFile[params.csv,3,constructType=param_val_file,col=param_val_csv]&quot;/&gt;</td>
</tr>
</tbody>
</table>

Figure 144 Snapshot of params_template.xls, Columns A-H

**Variables and their definitions**

Column A should remain a zero-indexed list of integers, incremented by one (1) for each row. This information is needed in the XML in Column H to tell construct what row the variable definition resides on.

Column B is the variable’s name. Construct does not allow spaces in variable names, nor to start with a numeric value. The example demonstrates an all lowercase style with words separated by underscores. As a matter of convention, I have maintained ascending alphabetical order for the variables in two groups: non-file name variables, and file name variables.

Column C is the value that the variable will assume in the params.csv file. The application that creates the directory structure for a virtual experiment as well as the data aggregator also uses the key-value pairs in Columns B & C.

Column D supports the generation of XML to define <var> elements in the input deck. Construct expects values to be “float”, “int”, “string”, and “bool.”

Column H is the XML definition of the <var> element that the researcher needs to manually copy this entire column into the input deck, overwriting the existing vars derived from params_template.xls.

**WARNING:** MS Excel copy and paste does not usually copy the MS-Excel escaped quotation marks in Column H into a text-only editor. A fast way to overcome this phenomena is to paste the material first into MS Word, then copy from MS Word the text to paste into the text-only editor.
Failure to copy and paste and ensure correct processing of escaped quotation marks may result in non-obvious deck failures!

Variables that impact <network> definitions

Columns E, F, and G store data needed to create a <network> element definition. A <network> is a collection of links between source and target nodes.

Column E is the type of node from which the link originates. It must be a value that construct expects and defined in the input deck’s <nodes> tree. In the example, the src node type is shown as agent.

<table>
<thead>
<tr>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>src</td>
<td>tgt</td>
<td>linktype</td>
<td>var</td>
<td>networks</td>
</tr>
</tbody>
</table>

Column F is the type of node to which the link connects. It must be a value that construct expects and defined in the input deck’s <nodes> tree. In the example, the tgt node type is an agent.

Column G is the link type. Construct expects this value to be one of the following: float, int, or bool. In the example, the linktype is a float in row 64 and bool in row 65.

Column H is, as discussed above for variables that do not impact network definitions, the XML definition of the <var> element. The researcher needs to manually copy this entire column into the input deck.

Column I is a visual separator and is not otherwise relevant.

Column J is a concatenation of Column K “Network Comment(s)” and Column L “additional network generators.” This concatenation reduces the number of columns the researcher needs to manually copy, into the input deck while supporting the possibility of
multiple network generators per network definition. The researcher needs to manually copy this entire column into the input deck, overwriting the existing <network> elements derived from params_template.xls.

**WARNING:** MS Excel copy and paste does not usually copy the MS-Excel escaped quotation marks in Column H into a text-only editor. A fast way to overcome this phenomena is to paste the material first into MS Word, then copy from MS Word the text to paste into the text-only editor.

**experiment_config_file.xls**

This file, as of April 2013, needs to remain in the pre-Excel 2007 format of .xls. 

*Warning: Do not use the .xlsx format, as the perl script processing the file uses a CPAN module that does not support the .xlsx format.*

This file is used by the makeCondorDirs script to setup the Box-Behnken experimental design. Each column represents a variable under test. The name of the variable must match exactly the variable name specified either in the deck or in the params_template.xls file. The second row is a comma-separated list of values that the variable can assume. Rows 3 and upwards (15 in the example above) are the values in the Box-Behnken design where -1 represents the lowest possible value from row 2, 0 represents the middle value from row 2, and 1 represents the highest value from row 2.
The `makeCondorDirs` script automatically reads and parses this file and applies its contents to the process of writing `params.csv` files for each of the experimental configurations under test.

The researcher must copy Columns H and J into the input deck if they have added or deleted any rows to the `params_template.xls` file. Failure to do update the input deck ensures the results will not reflect any changes to the template file!

### Updating Executables sent to the Condor cluster

The submission of jobs to the Condor cluster includes passing multiple executable files to each Condor node. Each of these executables must be up-to-date before the researcher creates the directories for the virtual experiment and submitting the jobs to Condor for execution.

In the `scriptsAndApps` folder, the following files must be **current:**

- `construct.exe` - the agent-based simulation executable
- `networkGenerator.jar` - the executable jar that will, on the condor client, read the `params.csv` file, and generate the various input networks that construct needs to run. For the multi-level resilience project, this is a highly specific application though the division of labor between numerous applications may remain appropriate for other projects, such as this dissertation.
- **dataAggregator.jar** - the executable jar that will, on the submitting machine, recursively traverse, reduce, and process the outputs of the condor jobs. Each condor client will return the results of the run (as specified in the construct input deck) *and anything else* in the condor working directory of the client.

In the *CondorPreparation* folder, the following files must be **current**:

- **condorShell.cmd** - this MS DOS script (using the cmd.exe found on various flavors of MS Windows operating systems since Windows XP) is the application that the condor client executes directly. It performs a multi-step process on each client

  - Confirms Perl and Java are installed on the condor client
  - Confirms that Perl is installed (Cygwin Perl)
    - if Perl is not installed, the script sets a flag to cause the network generator application to fail over to Java alternatives to the Perl Scripts
  - Confirms that 64-bit java is installed
    - Makes a critical assumption that the 64-bit java.exe is in `c:\program files\java` since Microsoft uses the `C:\Program Files (x86)` directory as the default location for 32-bit applications on 32-bit machines.
    - If 64-bit java is not installed, the script fails with an errorcode set to 1.
    - Just before exiting, the script creates a file called `64_Bit_JAVA_IS_MISSING_ON_%HOST%` and replaces `%HOST%` with the name of the machine. This file gets returned to the submitting machine and a post-processing script can support a researcher’s effort to identify and remediate machines without 64-bit java.
  - Note: 64-bit java has been necessary for several reasons
    - possibly sloppy coding that leads to heap and stack memory errors
    - insufficient heap and stack memory to process large quantities of large output files
  - Runs the **networkGenerator.jar** file
  - Run **construct** using **construct.xml** as the input
  - Deletes the input files and undesired output files.
  - Compresses the desired output files, then deletes the .csv versions
  - When the **condorShell.cmd** exits, the condor client transmits all the files in its working directory back to the submitting machine.

- **whichJVMIsInstalled.jar** - this Java application returns the highest version of installed JRE and JDK, if present, or an empty string if not present.

**Perl on submitting machine**

You must have Perl installed on the submitting machine. I’ve tested the scripts on cygwin perl 5.14.2. You must also have the following Perl Packages installed (CPAN comes in handy for this). All are installed on zurg.CASOS.cs.cmu.edu, the machine I usually submitted jobs from.
Directories for Condor Virtual Experiment

WARNING: The following steps need to be on a machine that can submit jobs to condor. If not, then the machine that can submit jobs to condor will need shared access to these folders and files to run.

The researcher should open a command prompt (cygwin is the shell prompt most used by the dissertation author) and change directory to the runs folder.

![Directory Structure](image)

Figure 147 Directory structure for construct runs

Execute `makeCondorDirs.pl` script (which of course presumes the reader has Perl installed on their system). The specific invocation syntax is below:

```bash
../../scriptsAndApps/CondorPreparation/makeCondorDirs.pl --verbose -best -p ../../construct/inputDecks/params_template.xls -c ../../construct/inputDecks/experiment_config_file.xls -i ../../construct/inputDecks/multiLevel_inputDeck.xml
```

`makeCondorDirs.pl --help` will show the options available for use as of April 2013.

Submitting to Condor for the Virtual Experiment

To submit to condor, assuming the condor client is installed and appropriately configured to submit to the condor cluster controller, enter the following command:

```
condor_submit condor_submission_file0000.txt
```

Alternatively, you can setup a for loop such as the one
for i in `ls condor_submission_file00*`; do condor_submit $i; done

The purpose of a five (5) minute delay between submissions is to allow some spacing of the file transmissions of the executables between the submitting client and the condor controller. It also spaces out the number of jobs on the controller at any given point. Finally, it spaces out the file transmissions from the executing condor client returning outputs to the submitting client.

**Post-Processing Outputs of Condor from a Virtual Experiment**

**Data Aggregation**

There are three ways to invoke the data aggregation. One is via an executable JAR file, the other is through Eclipse (assuming access to source code). The third is to have the aggregator run on the Condor Cluster. This recipe will review the running of the aggregator through Eclipse and then via the JAR file, and then the execution on the Condor Cluster.

**Data Aggregation via Eclipse IDE**

Assumption: The user has created a Java project within their Eclipse™ framework, and has the project correctly set to use Java 1.7 (there are reasons for using Java 1.7), java-getopt-1.0.14.jar as a Library in the Java Build Path.

Setup a *Run Configuration* using either the Run menu item or the drop down menu next to the run button as shown in the figure below.

![Figure 148 Eclipse's Run configurations menu item](image-url)
After selecting Run Configurations, the model should create or edit the run configuration for the data aggregator. If creating, you’ll want to click on the “Create Configuration” icon in the upper left corner, and if editing, you should see a window much like the one below. Ensure the Project name matches and the main class dialog box are correctly filled in.

You will also want to fill in the “Arguments” tab with the command line arguments as well as the working directory text box. The command line arguments are discussed below, and can be accessed using the command line execution environment with the -h option.

```
java -jar NetworkDataAggregator -h
```

Options, as of April 2013 are:

- `-f DirectoryName` Directories from Condor’s virtual experiment runs, naming convention has each starting with
  - `Condition_[int(s)]`
- `-v` verbose output
- `-d [ints >=1]` debug output of greater volume the higher the int
- `-o DirectoryName` Directory where the Aggregator will write output files

---

Figure 149 Eclipse run configuration for NetworkDataAggregator – main tab
The experimenter should also set the working directory to the same directory as the input directory. Once configured, the researcher can press “Apply” and “Close” and then invoke this run configuration at some future point in time.

**Data Aggregator from the Command Line**

Assuming the developer has exported a current and up-to-date copy of the executable JAR, the researcher can invoke it from the command line. For convenience, having the present working directory (pwd) as the input directory works well. The invocation is below:

```
java -jar NetworkDataAggregator -f inputDir [-v] [-d int] [-o outputDir]
```

If the output directory is not specified, the aggregator will write outputs to the present working directory.
Data Aggregation via Aggregator on Condor

Assuming the researcher has the outputs from the virtual experiment run available, aggregation on the Condor HPC is feasible.

The invocation for the Condor-based aggregator preparation program is shown below:

```
java -jar CondorBasedAggregator -f inputDir [-v] [-d int] [-o outputDir]
```

The outputs of this jar file will be a submission file per experimental condition as well as a series of .7z (7Zip) files that are the compressed outputs of the virtual experiment. The research may submit each condor submission file with an invocation like that shown below:

```
condor_submit condorBasedAggregation_0001.txt
```

Alternatively, you can setup a `for` loop such as the one shown below:

```
for i in `ls condorBasedAggregation_*`; do condor_submit $i; done
```

These condor jobs will transfer the compressed outputs of the virtual experiment directories. On the execute node, unzips the outputs, and processes the outputs. During processing it creates two (2) directories that Condor returns to the submitting node: AggregatorOutputs, and condition_00xx_AVG_Attributes.

To merge the results of these aggregator outputs into a single output file, use the bash script in the `CondorPostProcess` directory called `MergeAggregatorOutputs`. An example of invoking that shell script, from within the directory holding the results of the virtual experiment looks like this:

```
../../scriptsAndApps/CondorPostProcess/mergeAggregatorOutputs.sh
```

Using R for Graph Generation

Open R-Studio

Load “plotAllMetrics.r”

Change Line 4 “setwd” to match current run directory where aggregator data is stored

Change Line 8 if necessary
Change source lines 25 through 29 if necessary, which should be relative to the working directory

a. Set working dir in script if using IDE
Appendix 5 Construct Input Files

Parameters files

The table below is a listing of the parameter file used by the processing scripts and Construct. Electronic copies of the parameter file, the source code, and the executable jar file are available on my personal web page at http://www.andrew.cmu.edu/user/mlanham/dissertation/

Table 62: Parameters used to in operational and strategic simulations

<table>
<thead>
<tr>
<th>Line</th>
<th>Parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>a_attack_email_prob</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>a_attack_key_it_prob</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>a_attack_phone_prob</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>a_attack_web_prob</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>agent_flip_to_negative_rate</td>
<td>0.1</td>
</tr>
<tr>
<td>5</td>
<td>agent_flip_to_positive_rate</td>
<td>0.1</td>
</tr>
<tr>
<td>6</td>
<td>attack_end_time</td>
<td>41</td>
</tr>
<tr>
<td>7</td>
<td>attack_start_time</td>
<td>25</td>
</tr>
<tr>
<td>8</td>
<td>c_attack_prob</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>email_preference_mean</td>
<td>0.2</td>
</tr>
<tr>
<td>10</td>
<td>email_preference_variance</td>
<td>0.02</td>
</tr>
<tr>
<td>11</td>
<td>facetoface_preference_mean</td>
<td>0.6</td>
</tr>
<tr>
<td>12</td>
<td>facetoface_preference_variance</td>
<td>0.06</td>
</tr>
<tr>
<td>13</td>
<td>group_flip_to_positive_rate</td>
<td>0.1</td>
</tr>
<tr>
<td>14</td>
<td>group_flip_to_negative_rate</td>
<td>0.1</td>
</tr>
<tr>
<td>15</td>
<td>human_agent_forgetting_mean</td>
<td>0.99</td>
</tr>
<tr>
<td>16</td>
<td>human_agent_forgetting_rate</td>
<td>0.99</td>
</tr>
<tr>
<td>17</td>
<td>human_agent_forgetting_variance</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>human_agent_initiation_count</td>
<td>2</td>
</tr>
<tr>
<td>19</td>
<td>human_agent_learn_by_doing</td>
<td>0.75</td>
</tr>
<tr>
<td>20</td>
<td>human_agent_message_complexity</td>
<td>31</td>
</tr>
<tr>
<td>21</td>
<td>human_agent_reception_count</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>human_agent_selective_attention</td>
<td>0.9999</td>
</tr>
<tr>
<td>23</td>
<td>i_attack_prob</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>it_agent_initiation_count</td>
<td>2</td>
</tr>
<tr>
<td>25</td>
<td>it_agent_message_complexity</td>
<td>62</td>
</tr>
<tr>
<td>26</td>
<td>it_agent_reception_count</td>
<td>2</td>
</tr>
<tr>
<td>27</td>
<td>knowledge_count</td>
<td>3232</td>
</tr>
<tr>
<td>28</td>
<td>knowledge_general_count</td>
<td>2782</td>
</tr>
<tr>
<td>29</td>
<td>knowledge_plan_bad_count</td>
<td>150</td>
</tr>
<tr>
<td>30</td>
<td>knowledge_plan_count</td>
<td>300</td>
</tr>
<tr>
<td>31</td>
<td>knowledge_plan_priority</td>
<td>2</td>
</tr>
<tr>
<td>32</td>
<td>knowledge_priority</td>
<td>1</td>
</tr>
<tr>
<td>33</td>
<td>ktm_false_neg_rate</td>
<td>0.06</td>
</tr>
<tr>
<td>34</td>
<td>ktm_false_pos_rate</td>
<td>0.03</td>
</tr>
<tr>
<td>35</td>
<td>meeting_interaction_multiplier</td>
<td>3</td>
</tr>
<tr>
<td>36</td>
<td>meeting_plan_ratio</td>
<td>0.2</td>
</tr>
<tr>
<td>37</td>
<td>num_briefings</td>
<td>3</td>
</tr>
<tr>
<td>38</td>
<td>ora_input_fname</td>
<td>construct_ORA_file.xml</td>
</tr>
<tr>
<td>39</td>
<td>phone_preference_mean</td>
<td>0.1</td>
</tr>
<tr>
<td>40</td>
<td>phone_preference_variance</td>
<td>0.01</td>
</tr>
<tr>
<td>41</td>
<td>plan_briefing_1_end</td>
<td>22</td>
</tr>
<tr>
<td>Line</td>
<td>Parameter</td>
<td>value</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>42</td>
<td>plan_briefing_1_start</td>
<td>21</td>
</tr>
<tr>
<td>43</td>
<td>plan_briefing_2_end</td>
<td>34</td>
</tr>
<tr>
<td>44</td>
<td>plan_briefing_2_start</td>
<td>33</td>
</tr>
<tr>
<td>45</td>
<td>plan_briefing_3_end</td>
<td>46</td>
</tr>
<tr>
<td>46</td>
<td>plan_briefing_3_start</td>
<td>45</td>
</tr>
<tr>
<td>47</td>
<td>plan_briefing_duration</td>
<td>2</td>
</tr>
<tr>
<td>48</td>
<td>plan_briefing_interlude</td>
<td>11</td>
</tr>
<tr>
<td>49</td>
<td>plan_execution_ratio</td>
<td>0.3333</td>
</tr>
<tr>
<td>50</td>
<td>plan_time_count</td>
<td>27</td>
</tr>
<tr>
<td>51</td>
<td>social_proximity_weight</td>
<td>0.5</td>
</tr>
<tr>
<td>52</td>
<td>time_count</td>
<td>100</td>
</tr>
<tr>
<td>53</td>
<td>time_failover_complete</td>
<td>2</td>
</tr>
<tr>
<td>54</td>
<td>ttm_false_neg_rate</td>
<td>0.08</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Line</th>
<th>Parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>ttm_false_pos_rate</td>
<td>0.04</td>
</tr>
<tr>
<td>56</td>
<td>warm_up_period</td>
<td>20</td>
</tr>
<tr>
<td>57</td>
<td>warm_up_period_enabled</td>
<td>1</td>
</tr>
<tr>
<td>58</td>
<td>web_preference_mean</td>
<td>0.1</td>
</tr>
<tr>
<td>59</td>
<td>web_preference_variance</td>
<td>0.01</td>
</tr>
<tr>
<td>60</td>
<td>facetoiface</td>
<td>0</td>
</tr>
<tr>
<td>61</td>
<td>phone_lvl1</td>
<td>1</td>
</tr>
<tr>
<td>62</td>
<td>phone_lvl2</td>
<td>2</td>
</tr>
<tr>
<td>63</td>
<td>email_lvl1</td>
<td>3</td>
</tr>
<tr>
<td>64</td>
<td>email_lvl2</td>
<td>4</td>
</tr>
<tr>
<td>65</td>
<td>web_lvl1</td>
<td>5</td>
</tr>
<tr>
<td>66</td>
<td>web_lvl2</td>
<td>6</td>
</tr>
</tbody>
</table>
Construct input deck for operational and strategic simulation

<construct>
<!--
***************************************************************************** -->
<!-- GLOBAL VARIABLES -->
<!--***************************************************************************** -->
<construct_vars>
<!-- value is in col 1 (zero indexed) -->
<var name="param_val_col" value="1" /> 
<--
***************************************************************************** -->
<!-- Start vars from parameters file -->
<!-- copy 60+ var xml nodes from params_template.xls Column H -->
<!-- You may need to copy & paste into MS Word, then copy and paste into this XML document. It depends on how your XML editor handles the Excel-odities of embedded quotations in a cell -->
<--
***************************************************************************** -->
</construct>

<!-- a_attack_email_prob -->
<var name="a_attack_email_prob" value="readFromCSVFile[params.csv,0,construct::intvar::param_val_col]:float" />
<!-- a_attack_key_it_prob -->
<var name="a_attack_key_it_prob" value="readFromCSVFile[params.csv,1,construct::intvar::param_val_col]:float" />
<!-- a_attack_phone_prob -->
<var name="a_attack_phone_prob" value="readFromCSVFile[params.csv,2,construct::intvar::param_val_col]:float" />
<!-- a_attack_web_prob -->
<var name="a_attack_web_prob" value="readFromCSVFile[params.csv,3,construct::intvar::param_val_col]:float" />
<!-- agent_flip_to_negative_rate -->
<var name="agent_flip_to_negative_rate" value="readFromCSVFile[params.csv,4,construct::intvar::param_val_col]:float" />
<!-- agent_flip_to_positive_rate -->
<var name="agent_flip_to_positive_rate" value="readFromCSVFile[params.csv,5,construct::intvar::param_val_col]:float" />
<!-- c_attack_prob -->
<var name="c_attack_prob" value="readFromCSVFile[params.csv,8,construct::intvar::param_val_col]:float" />
<!-- email_preference_mean -->
<var name="email_preference_mean" value="readFromCSVFile[params.csv,9,construct::intvar::param_val_col]:float" />

</construct>
<var name="plan_time_count" value="readFromCSVFile[params.csv,50,construct::intvar::param_val_col]:int" />
<var name="social_proximity_weight" value="readFromCSVFile[params.csv,51,construct::intvar::param_val_col]:float" />
<var name="time_count" value="readFromCSVFile[params.csv,52,construct::intvar::param_val_col]:int" />
<var name="time_failover_complete" value="readFromCSVFile[params.csv,53,construct::intvar::param_val_col]:int" />
<var name="ttm_false_neg_rate" value="readFromCSVFile[params.csv,54,construct::intvar::param_val_col]:float" />
<var name="ttm_false_pos_rate" value="readFromCSVFile[params.csv,55,construct::intvar::param_val_col]:float" />
<var name="warm_up_period" value="readFromCSVFile[params.csv,56,construct::intvar::param_val_col]:int" />
<var name="warm_up_period_enabled" value="readFromCSVFile[params.csv,57,construct::intvar::param_val_col]:int" />
<var name="web_preference_mean" value="readFromCSVFile[params.csv,58,construct::intvar::param_val_col]:float" />
<var name="web_preference_variance" value="readFromCSVFile[params.csv,59,construct::intvar::param_val_col]:float" />
<var name="facetoface" value="readFromCSVFile[params.csv,60,construct::intvar::param_val_col]:int" />
<var name="phone_lvl1" value="readFromCSVFile[params.csv,61,construct::intvar::param_val_col]:int" />
<var name="phone_lvl2" value="readFromCSVFile[params.csv,62,construct::intvar::param_val_col]:int" />
<var name="email_lvl1" value="readFromCSVFile[params.csv,63,construct::intvar::param_val_col]:int" />
<var name="email_lvl2" value="readFromCSVFile[params.csv,64,construct::intvar::param_val_col]:int" />
<var name="web_lvl1" value="readFromCSVFile[params.csv,65,construct::intvar::param_val_col]:int" />
<var name="web_lvl2" value="readFromCSVFile[params.csv,66,construct::intvar::param_val_col]:int" />

<!-- deck calculated value instead of always checking the numerous vars that would indicate an attack: attack end time > 0; *_attack_*_prob > 0 used to include attack start time > 0, but there could be use cases where attacks start at time 0 -->
<var name="attack_enabled" value="if ((construct::floatvar::a_attack_email_prob > 0) ||
(construct::floatvar::a_attack_key_it_prob > 0)
|| (construct::floatvar::a_attack_phone_prob > 0)
|| (construct::floatvar::a_attack_web_prob > 0)
|| (construct::floatvar::c_attack_prob > 0)
|| (construct::floatvar::i_attack_prob > 0)
|| (construct::floatvar::a_attack_key_it_prob > 0)
|| (construct::intvar::attack_end_time > 0)){
    true
} else {
    false
}
" />
<!-- ############# end copy vars from
parameters file ############## -->

<var name="attack_time_list" value="construct::intvar::attack_start_time..construct::intvar::attack_end_time" />
<var name="attack_time_list_plus_one" value="construct::stringvar::attack_time_list,construct::intvar::attack_end_time+1" />
<var name="attacktime_output_list" value="(construct::intvar::attack_start_time-1)..construct::intvar::attack_end_time+1)" />

<var name="belief_count" value="0" />
<var name="CommunicationMedium_list" value="construct::intvar::facetoface..construct::intvar::web_lvl2" />
<var name="dummy_nodeclass_list" value="0" />
</var>
</var>
</var>
<var name="energytask_count" value="0" />

<var name="timeperiod_list" value="0..(construct::intvar::time_count - 1 )" />
<var name="plan_meeting_ticks" value="0..(construct::intvar::plan_briefing_duration-1)" />
<var name="meeting_id_list" value="0..(construct::intvar::num_briefings-1)" />
<var name="output_by_percentiles" value="\$
currTime\$ = 0;
$step$ = construct::intvar::time_count / 10; /* 10% step value, ASSUMES time_count >= 10 so $step$ >= (int)1 */
$result$ = '' + $currTime$;
foreach $i$ (timeperiod_list){
    if ($i$:int == ($currTime$ + $step$) ){
        $result$ = $result$ + ',' + ($currTime$ + $step$);
        $currTime$ = $i$:int;
    } else {
        $currTime$ = $currTime$; /* non-harm else
statement, since 'else' is not optional in
Construct's 'if then else' statements */
    }
} /* now add the last time period to the list */
$result$ = $result$ + ',' + (construct::intvar::time_count - 1);
return $result$;" with="$result$" />
<var name="plan_briefing_time_list" value="
$\text{plan\_briefing\_1\_time\_list}$=construct::intvar:plan\_briefing\_1\_start..construct::intvar:plan\_briefing\_1\_end;
$\text{plan\_briefing\_2\_time\_list}$=construct::intvar:plan\_briefing\_2\_start..construct::intvar:plan\_briefing\_2\_end;
$\text{plan\_briefing\_3\_time\_list}$=construct::intvar:plan\_briefing\_3\_start..construct::intvar:plan\_briefing\_3\_end;
$\text{result}$ = $\text{plan\_briefing\_1\_time\_list}$ + ',' + $\text{plan\_briefing\_2\_time\_list}$ + ',' + $\text{plan\_briefing\_3\_time\_list}$;
return $\text{result}$;
</construct\_vars>
<!--
******************************************************************************
*GLOBAL SIMULATION PARAMETERS****************************************************************************** -->
<!-- set to 1 for testing to ensure consistent output
@WARNING comment the line below for runs for record -->
<!-- <param name="seed" value="1.0" /> -->  
<!-- <param name="verbose\_initialization" value="true" /> -->  
<!-- <param name="verbose\_verification" value="true" /> -->  
<!-- <param name="verbose\_output\_timing" value="false" /> -->  
<!-- <param name="verbose\_interaction\_weights" value="false" /> -->  
<!-- <param name="active\_models" value="standard interaction model,standard task model" with="delay\_interpolation" /> -->  
<!-- <param name="active\_mechanisms" value="none" /> -->  
<!-- <param name="belief\_model" value="disable" /> -->  
<!-- <param name="binary\_forgetting" value="true" /> -->  
<!-- <param name="communicationWeight\_ForBelief" value="0.0" /> -->  
<!-- <param name="communicationWeight\_ForBeliefTM" value="0.0" /> -->  
<!-- <param name="communicationWeight\_ForFact" value="0.6" /> -->  
<!-- <param name="communicationWeight\_ForKnowledgeTM" value="0.4" /> -->  
<!-- <param name="communicationWeight\_ForBinaryTaskAssignment" value="0.0" /> -->  
<!-- <param name="communicationWeight\_ForBinaryTaskAssignmentTM" value="0.1" /> -->  
<!-- <param name="operation\_output\_working\_directory" value="'c:/Users/Michael.Lanham/Google_Drive/dissertation/construct/strategic'"/> -->  
<!-- <param name="default\_agent\_type" value="human" /> -->
<param name="dynamic_environment" value="false" />
<param name="forgetting" value="true" />
<param name="interaction_requirements" value="disable" />
<param name="thread_count" value="1" />
<param name="transactive_memory" value="enable" />
<param name="tm_model" value="multi_level" />
<param name="activation_threshold_agent" value="-1" />
<param name="activation_threshold_group" value="-2" />
<param name="agent_annealing_halflife" value="6" />
<param name="group_annealing_halflife" value="6" />
<param name="use_mail" value="false"/>
</construct_parameters>

<!-- Start groups' names and node IDs from parameters file -->
<!-- copy 30+ xml nodes from params_template.xlsx Sheet 'GroupNames' Column C -->
<!-- You may need to copy & paste into MS Word, then copy and paste # -->
<!-- into this XML document. It depends on how your XML editor handles ## -->
<!-- the Excel-oddities of embedded quotations in a cell -->
<nodeclass type="agent" id="agent"> <!-- id serves as the prefix to the counter for node IDs -->
<properties>
    <property name="generate_nodeclass" value="true" />
    <property name="generator_type" value="dynetml" />
    <property name="generator_doc_path" value="construct::stringvar::ora_input_fname" />
    <property name="generator_nodeclass_id" value="agent" />
</nodeclass>

<!-- mandatory non-empty nodeclass read from Strategic model DynetML file-->
<!-- mandatory non-empty nodeclass read from Strategic model DynetML files, uses organization node set-->

<nodeclass type="agentgroup"
 id="agentgroup">

<properties>

<property name="generate_nodeclass"
 value="true" />

<property name="verbose" value="true" />

<property name="generator_type"
 value="dynetml"/>

<property name="generator_doc_path"
 value="construct::stringvar::ora_input_fname" />

<property name="generator_nodeclass_id"
 value="organization" />

<property name="generator_nodeclass_type"
 value="Organization" />

</properties>

</nodeclass>

<nodeclass type="agent_type"
 id="agent_type">

<node id="human" title="human">

<properties>

<property name="communicationMechanism"
 value="direct" />

<property name="canSendCommunication"
 value="true" />

<property name="canReceiveCommunication"
 value="true" />

<property name="canSendKnowledge"
 value="true" />

<property name="canReceiveKnowledge"
 value="true" />

</nodeclass>
<property name="canReceiveBeliefsTM" value="false" />
<!-- beliefs not part of lanham's dissertation -->
</properties>
</node>
<node id="it" title="it">
<properties>
  <property name="communicationMechanism" value="direct" />
  <property name="canSendCommunication" value="true" />
  <property name="canReceiveCommunication" value="true" />
  <property name="canSendKnowledge" value="true" />
  <property name="canReceiveKnowledge" value="true" />
  <property name="canSendBeliefs" value="false" />
  <property name="canReceiveBeliefs" value="false" />
  <property name="canSendBeliefsTM" value="false" />
  <property name="canReceiveBeliefsTM" value="false" />
  <property name="canSendBinaryTaskAssignment" value="false" />
  <property name="canReceiveBinaryTaskAssignment" value="false" />
  <property name="canSendBinaryTaskAssignmentTM" value="false" />
  <property name="canReceiveBinaryTaskAssignmentTM" value="false" />
</properties>
</node>
<nodeclass type="CommunicationMedium" id="CommunicationMedium">
<properties>
  <property name="generate_nodeclass" value="true" />
  <property name="verbose" value="true" />
  <property name="generator_type" value="dynetml" />
  <property name="generator_doc_path" value="construct::stringvar::ora_input_fname" />
  <property name="generator_nodeclass_id" value="comms_media" />
  <property name="generator_nodeclass_type" value="Resource" />
</properties>
</nodeclass>
<nodeclass type="knowledge" id="knowledge">
<properties>
</properties>
</nodeclass>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path" value="construct::stringvar::ora_input_fname"/>
<property name="generator_nodeclass_id" value="knowledge" />
<property name="generator_nodeclass_type" value="knowledge" />
</nodeclass>

<nodeclass type="knowledgegroup" id="knowledgegroup">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path" value="construct::stringvar::ora_input_fname"/>
<property name="generator_nodeclass_id" value="knowledgegroup" />
<property name="generator_nodeclass_type" value="unknown" />
</properties>
</nodeclass>

<nodeclass type="binarytask" id="binarytask">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="dynetml"/>
<property name="generator_doc_path" value="construct::stringvar::ora_input_fname"/>
<property name="generator_nodeclass_id" value="task" />
<property name="generator_nodeclass_type" value="task" />
</properties>
</nodeclass>

<nodeclass type="timeperiod" id="timeperiod">
<properties>
<property name="generate_nodeclass" value="true" />
<property name="generator_type" value="count" />
<property name="generator_count" value="construct::intvar::time_count" />
</properties>
</nodeclass>

<nodeclass type="dummy_nodeclass" id="dummy_nodeclass">
<node id="constant" title="constant" />
</nodeclass>

<networks>
<!-- need these first two grouping networks defined early, as they are used in a lot of the generators -->
<network src_nodeclass_type="agent" target_nodeclass_type="agentgroup" id="agent"/>
group membership network" link_type="bool"
  network_type="dense">
  <!-- need to assign agents to one or more
  groups within the simulation -->
  <!-- Load from File -->
  <generator type="dynetml">
    <param name="filesystem_path"
      value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="'agent x organization'" />
    <param name="transpose" value="false" />
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::agentgroup::count_minus_one" />
    <param name="verbose" value="false" />
  </generator>
</network>

<network src_nodeclass_type="knowledge"
target_nodeclass_type="knowledgegroup"
id="knowledge group membership network"
link_type="bool" network_type="dense">
  <generator type="dynetml">
    <!-- @warning note the use of single quotes
    to force construct to treat
    the 'value' as an entire string, else
    the : and \ cause the Construct lexer fits !-->
    <param name="filesystem_path"
      value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="'knowledge x knowledgegroup'" />
    <param name="transpose" value="false" />
    <rows first="0" last="nodeclass::knowledge::count_minus_one" />
    <cols first="0" last="nodeclass::knowledgegroup::count_minus_one" />
    <param name="verbose" value="false" />
  </generator>
</network>

<!-- remainder of networks are in alphabetical
order by network name/id

**********************************************************************
remainder of networks are in alphabetical
order by network name/id
**********************************************************************>

<network src_nodeclass_type="agent"
target_nodeclass_type="agent"
id="access network"
link_type="float" network_type="dense">
  <generator type="dynetml">
    <param name="filesystem_path"
      value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="'agent x agent'" />
    <param name="transpose" value="false" />
  </generator>
</network>
<!-- connect integrity agent to Key IT Agents with specified probability -->
<generator type="randombinary">

<!-- causes seg faults -->
<rows groups="integrity_agent_level2_group" 
    group_membership_network="agent group membership network" />
<cols groups="it_agent_key_level2_group" 
    group_membership_network="agent group membership network" />
<param name="mean" 
    value="construct::floatvar::i_attack_prob" />
<!--<param name="density" value="0.05" /-->  
<!-- for use with erdos_renyi -->
</generator>
</network>
ll_spare_group, it_agent_key_level2_spare_group, confidentiality_sink_group" group_membership_network="'agent group membership network'" />
<cols first="0" last="nodeclass::timeperiod::count_minus_one" />
<param name="constant_value" value="0.0" />
</generator>
<!-- during attacks, integrity agents get turned on, key agents get turned off, and spare agents get turned on-->
<!-- turn integrity agent on at specified prob during 'attack' times -->
<generator type="randombinary">
<rows groups="integrity_agent_group" group_membership_network="'agent group membership network'" />
<cols values="attack_time_list" />
<param name="mean" value="construct::floatvar::i_attack_prob" />
</generator>
<!-- turned off 80% is the same as turned on 20%-->
<rows groups="it_agent_key_level2_group, it_agent_key_level2_group" group_membership_network="'agent group membership network'" />
<cols values="attack_time_list" />
<param name="mean" value="1-construct::floatvar::a_attack_key_it_prob" />
</generator>
<!-- if a Key IT attack is 'on', turn spare key IT on with specified delay (time_failover_complete) as an integer multiplier of a (plan + brief) cycle, once turned on during an attack, spare IT systems stay on until end of simulation -->
<generator type="constant">
<rows groups="it_agent_key_level1_spare_group, it_agent_key_level2_spare_group" group_membership_network="'agent group membership network'" />
<cols values="" $spares_on$ = '0';
if (construct::intvar::a_attack_key_it_prob > 0.0) {
  $spares_on$ = (construct::intvar::attack_start_time +
  (construct::intvar::time_failover_complete*
  (construct::intvar::plan_briefing_duration +
  construct::intvar::plan_briefing_interlude)))..nodeclass::timeperiod::count_minus_one;
} else {
  $spares_on$ = '0';
}
return $spares_on$;" />
<param name="constant_value" value="1.0" />
</generator>
<!-- when confidentiality attacks are enabled, turn the sink(s) on probabilistically for the entire run -->
<generator type="randombinary">
<rows groups="confidentiality_sink_group" group_membership_network="'agent group membership network'" />
<cols values="" />
<param name="constant_value;" value="1.0" />
</generator>
<cols values="0..nodeclass::timeperiod::count_minus_one" />

<param name="mean" value="construct::floatvar::c_attack_prob" />
</generator>

</network>

<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="agent
initiation count network" link_type="int" network_type="dense">
 <!-- Assign number of initiations per turn per agent -->
 <!-- default values for all agents -->
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::timeperiod::count_minus_one" />
<param name="constant_value" value="construct::intvar::human_agent_initiation_count" />
</generator>

<!-- confidentiality agent is a sink, and does not initiate interactions but does receive interactions -->
<generator type="constant">
<rows groups="confidentiality_sink_group" group_membership_network="agent group membership network!" />
<cols first="0" last="nodeclass::timeperiod::count_minus_one" />
<param name="constant_value" value="0" />
</generator>

<!-- Integrity agents are IT agents and initiations per turn are the same as IT agents.. -->
<!-- JPG briefers in meetings get to talk more -->
<generator type="constant">
<rows groups="jpg_joint_planning_group" group_membership_network="agent group membership network!" />
<cols values="meeting_time_list" />
<param name="constant_value" value="construct::intvar::human_agent_initiation_count * construct::intvar::meeting_interaction_multiplier" />
</generator>

</network>
message complexity network" link_type="int"
  network_type="dense">
  <!-- Assign complexity of messages per agent
  per time period -->
  <!--default values -->
  <generator type="constant">
    <rows first="0"
      last="nodeclass::agent::count_minus_one" />
    <cols first="0"
      last="nodeclass::timeperiod::count_minus_one"
    />
    <param name="constant_value"
      value="construct::intvar::human_agent_message_complexity" />
  </generator>
  <!-- set default IT Systems, which can
  send/receive more complex messages -->
  <generator type="constant">
    <rows groups="it_agent_group"
      group_membership_network="'agent group membership network'" />
    <cols first="0"
      last="nodeclass::timeperiod::count_minus_one"
    />
    <param name="constant_value"
      value="construct::intvar::it_agent_message_complexity" />
  </generator>
  <!-- JPG attendees in meetings get to listen
  more -->
  <generator type="constant">
    <rows groups="jpg_briefing"
      group_membership_network="'agent group membership network'" />
    <cols values="meeting_time_list"
      last="nodeclass::timeperiod::count_minus_one"
    />
    <param name="constant_value"
      value="construct::intvar::human_agent_reception_count * 
      construct::intvar::meeting_interaction_multiplier" />
  </generator>
</network>
<!-- integrity agents don't listen to anybody -->

<generator type="constant">
  <rows groups="integrity_agent_group" group_membership_network="agent_group membership network" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="0" />
</generator>

<network src_nodeclass_type="agent" target_nodeclass_type="knowledge" id="agent forgetting rate network" link_type="float" network_type="dense">
  <generator type="randomuniform">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::knowledge::count_minus_one" />
    <param name="min" value="if ((construct::floatvar::human_agent_forgetting_rate-(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else {construct::floatvar::human_agent_forgetting_rate-(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="max" value="if ((construct::floatvar::human_agent_forgetting_rate+(3.0*construct::floatvar::human_agent_forgetting_variance)) > 1.0) {1.0} else {construct::floatvar::human_agent_forgetting_rate+(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass" id="agent forgetting mean network" link_type="float" network_type="dense">
  <generator type="randomuniform">
    <rows first="0" last="0" />
    <cols first="0" last="0" />
    <param name="min" value="if ((construct::floatvar::human_agent_forgetting_mean-(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else {construct::floatvar::human_agent_forgetting_mean-(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="max" value="if ((construct::floatvar::human_agent_forgetting_mean+(3.0*construct::floatvar::human_agent_forgetting_variance)) > 1.0) {1.0} else {construct::floatvar::human_agent_forgetting_mean+(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass" id="agent forgetting mean network" link_type="float" network_type="dense">
  <generator type="randomuniform">
    <rows first="0" last="0" />
    <cols first="0" last="0" />
    <param name="min" value="if ((construct::floatvar::human_agent_forgetting_mean-(3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else {construct::floatvar::human_agent_forgetting_mean-(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="max" value="if ((construct::floatvar::human_agent_forgetting_mean+(3.0*construct::floatvar::human_agent_forgetting_variance)) > 1.0) {1.0} else {construct::floatvar::human_agent_forgetting_mean+(3.0*construct::floatvar::human_agent_forgetting_variance)}"/>
    <param name="symmetric_flag" value="false" />
  </generator>
</network>
id="agent forgetting variance network"
link_type="float" network_type="dense">
  <generator type="randomuniform">
    <rows first="0" last="nodeclass::agent::count_minus_one"/>
    <cols first="0" last="0"/>
    <param name="min" value="if
    (3.0*construct::floatvar::human_agent_forgetting_variance
    - (3.0*construct::floatvar::human_agent_forgetting_variance)) < 0.0) {0.0} else
    {3.0*construct::floatvar::human_agent_forgetting_variance}="/>
    <param name="max" value="if
    (3.0*construct::floatvar::human_agent_forgetting_variance) > 1.0) {1.0} else
    {3.0*construct::floatvar::human_agent_forgetting_variance}="/>
    <param name="symmetric_flag" value="false"/>
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass" id="agent learning rate network" link_type="float" network_type="dense">
  <generator type="randomuniform">
    <rows first="0" last="nodeclass::agent::count_minus_one"/>
    <cols first="0" last="0"/>
    <param name="min" value="if
    (construct::floatvar::human_agent_learn_by_doing > 0.5) {1.0-
     construct::floatvar::human_agent_learn_by_doing } else
    {construct::floatvar::human_agent_learn_by_doing}="/>
    <param name="max" value="if
    (construct::floatvar::human_agent_learn_by_doing > 0.5) {1.0-
     construct::floatvar::human_agent_learn_by_doing } else {1.0-
     construct::floatvar::human_agent_learn_by_doing}="/>
    <param name="symmetric_flag" value="false"/>
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass" id="agent selective attention effect network" link_type="float" network_type="dense">
  <generator type="constant">
    <rows first="0" last="nodeclass::agent::count_minus_one"/>
    <param name="min" value="1.0-
     construct::floatvar::human_agent_learn_by_doing "/>
    <param name="max" value="construct::floatvar::human_agent_learn_by_doing="/>
</network>
<!-- random values for human agent in the absence of empirical data -->
<generator type="randomnormal">
  <rows groups="it_agent_group"
group_membership_network="'agent group membership network'" />
  <cols first="0"
last="nodeclass::timeperiod::count_minus_one" />
  <param name="mean" value="0.01" />
  <param name="variance" value="0.05" />
</generator>

<!-- Access each agent access to one or more communications mediums. Without access to >= 1, the agent cannot communicate with anyone -->
<generator type="dynetml">
  <param name="filesystem_path"
value="construct::stringvar::ora_input_fname" />
  <param name="network_name" value="'agent x comms_media'" />
  <param name="transpose" value="false" />
  <rows first="0"
last="nodeclass::agent::count_minus_one" />
  <cols first="0"
last="nodeclass::CommunicationMedium::count_minus_one" />
  <param name="network_name" value="'knowledge x task'" />
  <param name="transpose" value="false" />
  <rows first="0"
last="nodeclass::agent::count_minus_one" />
  <cols first="0"
last="nodeclass::binarytask::count_minus_one" />
</generator>
</generator>
</network>

<network src_nodeclass_type="agent"
inner_nodeclass_type="agent"
target_nodeclass_type="CommunicationMedium"
id="communication medium preferences network 3d" link_type="float" network_type="dense3d">
  <!-- IT systems on level 1 can only use web to talk with other level 1 systems -->
  <generator type="constant3d">
    <rows groups="it_agent_level1_group"
      group_membership_network=""agent group membership network!"" />
    <inners groups="it_agent_level1_group,human_agent_group"
      group_membership_network=""agent group membership network!"" />
    <cols values="web_lvl1" />
    <param name="constant_value" value="1.0" />
  </generator>
  <!-- human agents prefer face-to-face with each other X% of the time -->
  <generator type="constant3d">
    <rows groups="human_agent_group"
      group_membership_network=""agent group membership network!"" />
    <inners groups="human_agent_group"
      group_membership_network=""agent group membership network!"" />
    <cols values="facetoface" />
    <param name="constant_value" value="construct::floatvar::facetoface_preference_mean" />
  </generator>
</network>

<!-- IT systems on level 2 can only use web to talk with other level 2 systems -->
<generator type="constant3d">
  <rows groups="it_agent_level2_group"
    group_membership_network=""agent group membership network!"" />
  <inners groups="it_agent_level2_group,human_agent_level2_group"
    group_membership_network=""agent group membership network!"" />
  <cols values="web_lvl2" />
  <param name="constant_value" value="1.0" />
</generator>

<!-- human agents when talking to themselves are assured of access via facetoface-->
<generator type="constantdiagonal3d">
  <rows groups="human_agent_group"
    group_membership_network=""agent group membership network!"" />
  <inners groups="human_agent_group"
    group_membership_network=""agent group membership network!"" />
  <cols values="facetoface" />
  <param name="constant_value" value="1.0" />
</generator>

<!-- web interaction is the only choice to interact with IT systems as the target/alter-->
</generator>
human agents prefer phone & email (unfiltered & filtered) with each other Y% of the time, respectively
@TODO fix this so its collocation, non-collocation sensitive

human agents prefer web (unfiltered & filtered) with each other \(Z\%\) of the time, respectively

@TODO fix this so its collocation, non-collocation sensitive -->

human agents prefer web (unfiltered & filtered) with each other \(Z\%\) of the time, respectively

@TODO well...this may be too extreme because they may not talk to non-plan aware people which is bad during the briefing periods -->
<!--default values -->
<generator type="constant">
  <rows groups="jpg_joint_planning_group"
group_membership_network="agent group membership network" />
  <cols
groups="plan_k_level1,plan_k_level2,bad_plan_k_level1,bad_plan_k_level2"
group_membership_network="knowledge group membership network" />
  <param name="constant_value" value="construct::intvar::knowledge_plan_priority" />
</generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="agent"
id="interaction sphere network" link_type="bool" network_type="dense">
  <!-- starting absolute agent x agent interaction network -->
  <generator type="dynetml">
    <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
    <param name="network_name" value="agent x agent" />
    <param name="transpose" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
id="knowledge expertise weight network" link_type="float" network_type="dense">
  <!-- weight each ego gives to knowledge bits it does not have when deciding which alter to interact with -->
  <generator type="randomuniform">
    <rows first="0" last="nodeclass::agent::count_minus_one" />
    <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
    <param name="min" value="0.4" />
    <param name="max" value="0.9" />
  </generator>
  <generator type="randomuniform">
    <rows groups="jpg_joint_planning_group,jpg_briefing"
group_membership_network="agent group membership network" />
    <cols values="construct::stringvar::plan_meeting_ticks" />
    <param name="min" value="0.8" />
    <param name="max" value="0.9999" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
id="knowledge network" link_type="float" network_type="dense">
  <!-- agent x knowledge assignment -->
</network>
<!-- Load from File -->
<generator type="dynetml">
  <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
  <param name="network_name" value="'agent x knowledge'" />
  <param name="transpose" value="false" />
  <rows first="0" last="nodeclass::agent::count_minus_one" />
  <cols first="0" last="nodeclass::knowledge::count_minus_one" />
</generator>
<!-- insert level 1 plan data into all Key IT systems with high density erdos renyi -->
<generator type="randomnormal">
  <rows groups="it_agent_key_group" group_membership_network="'agent group membership network'" />
  <cols groups="plan_k_level1" group_membership_network="'knowledge group membership network'" />
  <param name="mean" value="0.8" />
  <param name="variance" value="0.08" />
</generator>
<!-- insert level 1 plan data into JPG with lower density erdos renyi, as orders come through electronically -->
<generator type="randomnormal">
  <rows groups="jpg_joint_planning_group" group_membership_network="'agent group membership network'" />
  <cols groups="plan_k_level1" group_membership_network="'knowledge group membership network'" />
  <param name="mean" value="0.2" />
  <param name="variance" value="0.08" />
</generator>
<!-- insert level 2 plan data into level 2 Key IT systems with high density erdos renyi, as orders come through electronically -->
<!-- 28 Mar 15, erdos renyi generate was causing a seg fault when row count != col count so moved back to random normal generator-->
<generator type="randomnormal">
  <rows groups="it_agent_key_level2_group" group_membership_network="'agent group membership network'" />
  <cols groups="plan_k_level2" group_membership_network="'knowledge group membership network'" />
  <param name="mean" value="0.8" />
  <param name="variance" value="0.08" />
</generator>
<!-- insert level 2 plan data into JPG with lower density erdos renyi, as orders come through electronically -->
<!-- 28 Mar 15, erdos renyi generate was causing a seg fault when row count != col count so moved back to random normal generator-->
<generator type="randomnormal">
  <rows groups="jpg_joint_planning_group" group_membership_network="'agent group membership network'" />
  <cols groups="plan_k_level2" group_membership_network="'knowledge group membership network'" />
  <param name="mean" value="0.2" />
  <param name="variance" value="0.08" />
</generator>
<!-- insert level 2 plan data into JPG with lower density erdos renyi, as orders come through electronically -->
<!-- 28 Mar 15, erdos renyi generate was causing a seg fault when row count != col count so moved back to random normal generator-->
<generator type="randomnormal">
  <rows groups="jpg_joint_planning_group" group_membership_network="'agent group membership network'" />
  <cols groups="plan_k_level2" group_membership_network="'knowledge group membership network'" />
  <param name="mean" value="0.2" />
  <param name="variance" value="0.08" />
</generator>
<generator>
  <network src_nodeclass_type="agent" target_nodeclass_type="knowledge" id="learnable knowledge network" link_type="bool" network_type="dense">
    <generator type="constant">
      <!-- all knowledge is learnable -->
      <rows first="0" last="nodeclass::agent::count_minus_one" />
      <cols first="0" last="nodeclass::knowledge::count_minus_one" />
      <param name="constant_value" value="1" />
    </generator>
  </network>
  <network src_nodeclass_type="CommunicationMedium" target_nodeclass_type="knowledge" id="medium knowledge group network" link_type="bool" network_type="dense">
    <!-- CommunicationMedium x knowledge group assignment...iow, which groups do the mediums support? -->
    <!-- @TODO Fix this so knowledge is not controlled in such an absolutist manner
    <!-- it is more likely that all knowledge groups can go over all communications/media -->
    <!-- In the mean time, load from File the network manually constructed in the ORA file-->
    <generator type="dynetml">
      <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
      <param name="network_name" value="physical proximity network" />
      <param name="transpose" value="true" />
    </generator>
  </network>
  <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod" id="physical proximity weight network" link_type="float" network_type="dense">
    <!-- proximity of agents to each other. Zero(0) ==> maximally distant with each other with one(1)==>maximally close -->
    <generator type="dynetml">
      <param name="filesystem_path" value="construct::stringvar::ora_input_fname" />
      <param name="network_name" value="physical proximity" />
      <param name="transpose" value="false" />
    </generator>
  </network>
</generator>
<!-- default values -->
<generator type="randomnormal">
  <rows first="0" last="nodeclass::agent::count_minus_one" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="mean" value="0.6" />
  <param name="variance" value="0.06" />
</generator>
<generator type="constant">
  <rows groups="it_agent_group" group_membership_network="'agent group membership network'" />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="constant_value" value="0.0" />
</generator>
<generator type="randomnormal">
  <rows groups="jpg_joint_planning_group,jpg_briefing" group_membership_network="'agent group membership network'" />
  <cols values="construct::stringvar::plan_briefing_time_list" />
  <param name="mean" value="0.8" />
  <param name="variance" value="0.02" />
</generator>
</network>

<!-- Not used in this model, so all zeros -->
<generator type="constant">
  <rows first="0" last="nodeclass::agent::count_minus_one" />
  <cols first="0" last="nodeclass::dummy_nodeclass::count_minus_one" />
  <param name="constant_value" value="0.0" />
</generator>

<generator type="constant">
  <rows groups="it_agent_group" group_membership_network="'agent group membership network'" />
  <cols groups="it_agent_group" group_membership_network="'agent group membership network'" />
  <param name="constant_value" value="0.0" />
</generator>

<generator type="randomuniform">
  <rows groups="human_agent_group" group_membership_network="'agent group membership network'" />
  <cols groups="human_agent_group" group_membership_network="'agent group membership network'" />
  <param name="min" value="0.05" />
  <param name="max" value="0.90" />
</generator>

<!-- random values for human agent in the absence of empirical data -->
<generator type="randomuniform">
  <rows groups="human_agent_group" group_membership_network="'agent group membership network'" />
  <cols groups="human_agent_group" group_membership_network="'agent group membership network'" />
  <param name="min" value="0.05" />
  <param name="max" value="0.90" />
</generator>
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols first="0" last="nodeclass::agent::count_minus_one"/>
<param name="constant_value" value="0.0"/>
</generator>

<generator type="randomnormal">
<rows groups="human_agent_group" group_membership_network=""agent group membership network""/>
<cols groups="human_agent_group" group_membership_network=""agent group membership network""/>
<param name="mean" value="0.4"/>
<param name="variance" value="0.15"/>
</generator>

<generator type="constant">
<rows first="0" last="nodeclass::timeperiod::count_minus_one"/>
<cols first="0" last="nodeclass::timeperiod::count_minus_one"/>
<param name="constant_value" value="0.0"/>
</generator>

<!-- default value = 0 for all agents-->
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols first="0" last="nodeclass::agent::count_minus_one"/>
<param name="constant_value" value="0.0"/>
</generator>

<!-- random values for human agent in the absence of empirical data -->
<generator type="randomnormal">
<rows groups="human_agent_group" group_membership_network=""agent group membership network""/>
<cols groups="human_agent_group" group_membership_network=""agent group membership network""/>
<param name="mean" value="0.4"/>
<param name="variance" value="0.15"/>
</generator>

<!-- default value = 0 for all agents-->
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols first="0" last="nodeclass::agent::count_minus_one"/>
<param name="constant_value" value="0.0"/>
</generator>

<!-- when picking an interaction partner, weight ego uses to develop probability of interaction -->
<!-- default value = 0 for all agents-->
<generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one"/>
<cols first="0" last="nodeclass::timeperiod::count_minus_one"/>
<param name="constant_value" value="0.0"/>
</generator>
<!-- random values for human agent in the absence of empirical data -->
<generator type="randomnormal">
  <rows groups="human_agent_group"
group_membership_network=\'agent group membership network\' />
  <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
  <param name="mean" value="0.6" />
  <param name="variance" value="0.06" />
</generator>

<generator type="constant">
  <rows first="0" last="nodeclass::agent::count_minus_one" />
  <cols first="0" last="nodeclass::knowledge::count_minus_one" />
  <param name="constant_value" value="construct::intvar::knowledge_priority" />
</generator>

<!-- when picking knowledge to transmit to alters, weight assigned to each knowledge bit for inclusion in messages -->
<generator type="constant">
  <rows first="0" last="nodeclass::knowledge::count_minus_one" />
  <cols first="0" last="nodeclass::agent::count_minus_one" />
  <param name="constant_value" value="construct::intvar::knowledge_priority" />
</generator>

<!-- integrity agents like to transmit nothing but bad plan knowledge -->
<generator type="constant">
  <rows groups="integrity_agent_group, jpg_briefing"
group_membership_network=\'agent group membership network\' />
  <cols first="0" last="nodeclass::knowledge::count_minus_one" />
  <param name="constant_value" value="0" />
</generator>

<generator type="constant">
  <rows groups="integrity_agent_group, jpg_briefing"
group_membership_network=\'agent group membership network\' />
  <cols first="0" last="nodeclass::knowledge::count_minus_one" />
  <param name="constant_value" value="construct::intvar::knowledge_plan_priority" />
</generator>

<generator type="constant">
  <rows groups="jpg_joint_planning_group, jpg_briefing"
group_membership_network=\'agent group membership network\' />
  <cols groups="plan_k_level1, plan_k_level2, bad_plan_k_level1, bad_plan_k_level2"
group_membership_network=\'knowledge group membership network\' />
  <param name="constant_value" value="construct::intvar::knowledge_plan_priority" />
</generator>

<generator type="constant">
  <rows groups="bad_plan_k_level1, bad_plan_k_level2"
group_membership_network=\'knowledge group membership network\' />
  <cols groups="plan_k_level1, plan_k_level2, bad_plan_k_level1, bad_plan_k_level2"
group_membership_network=\'knowledge group membership network\' />
  <param name="constant_value" value="construct::intvar::knowledge_plan_priority" />
</generator>

</network>
<networks/>

<!--
******************************************************************************
********** INITIAL TRANSACTIVE MEMORY VALUES -->

<transactivememory
<!-- default random values created from
random_value < false positive and negative
rates and omniscient knowledge value -->
<network id="knowledge transactive memory
network" ego_nodeclass_type="agent"
src_nodeclass_type="agent"
target_nodeclass_type="knowledge"
link_type="bool" network_type="TMBool"
associated_network="knowledge network">
<!-- shifted away from perception based to
group based for use with multi-level TM -->
<!-- <generator type="perception_based">
<ego
values="construct::agentgroupvar::all_non_integ
rity_agents" />
<alter
values="construct::agentgroupvar::all_non_integ
rity_agents" />
<transactive
values="construct::knowledgegroupvar::no_bad_k"
/></generator>

<generator type="group_based">
<ego first="0"
last="nodeclass::agent::count_minus_one"/>
<alter first="0"
last="nodeclass::agent::count_minus_one"/>
<transactive first="0"
last="nodeclass::knowledge::count_minus_one"/>
<param name="name"
value="initial_KTM_all_non_integrity_agents_and
_all_non_bad_knowledge" />
<param name="false_positive_rate"
value="construct::floatvar::ktm_false_pos_rate" />
<param name="false_negative_rate"
value="construct::floatvar::ktm_false_neg_rate" />
<param name="rounding_threshold" value="0.0" />
<param name="verbose" value="true" />
<param name="verbosity_frequency"
value="50" />
<!{1}** display every nth
agent**{1}>
</generator>

<generator type="group_based">
<ego
values="construct::agentgroupvar::all_non_integ
rity_agents" />
<alter
values="construct::agentgroupvar::all_non_integ
rity_agents" />
<transactive
values="construct::knowledgegroupvar::no_bad_k"
/>
<param name="agent_flip_to_negative_rate" value="construct::floatvar::agent_flip_to_negative_rate"/>
<param name="verbose" value="true"/>
</generator>

</network>
<network id="binarytask transactive memory network" ego_nodeclass_type="agent" src_nodeclass_type="agent" target_nodeclass_type="binarytask" link_type="bool" network_type="TMBool" associated_network="binarytask assignment network">
<!-- shifted away from perception based to group based for use with multi-level TM -->
<!-- <generator type="perception_based">
<ego values="construct::agentgroupvar::all_non_integrity_agents" />
<alter values="construct::agentgroupvar::all_non_integrity_agents" />
<transactive first="0" last="nodeclass::binarytask::count_minus_one" />
<param name="name" value="initial_BinaryTaskTM_all_non_integrity_agents_and_all_binary_tasks" />
<param name="false_positive_rate" value="construct::floatvar::ttm_false_pos_rate"/>
<param name="false_negative_rate" value="construct::floatvar::ttm_false_neg_rate"/>
</generator>
-->
<generator type="group_based">
<ego first="0" last="nodeclass::agent::count_minus_one"/>
<alter first="0" last="nodeclass::agent::count_minus_one"/>
<transactive first="0" last="nodeclass::knowledge::count_minus_one" />
<param name="name" value="initial_BinaryTaskTM_group_to_group" />
<param name="group_flip_to_positive_rate" value="construct::floatvar::group_flip_to_positive_rate"/>
<param name="group_flip_to_negative_rate" value="construct::floatvar::group_flip_to_negative_rate"/>
<param name="agent_flip_to_positive_rate" value="construct::floatvar::agent_flip_to_positive_rate"/>
<param name="agent_flip_to_negative_rate" value="construct::floatvar::agent_flip_to_negative_rate"/>
<param name="verbose" value="true"/>
</generator>
</network>
<transactivememory>
<!-- OPERATIONS FOR SIMULATION OUTPUT -->
<!-- these are the values that are printed and/or saved -->
<!-- these operations help test that Construct read the node sets of the dynetml file correctly -->

<!-- Output operations intended for debugging...supports modelers' effort to compare as designed with as implemented -->

<!-- these operations help test that Construct read the node sets of the dynetml file correctly -->

<!-- Nodeset_dump -->
<operations>
<!-- Nodeset_dump -->
<operation name="Nodeset_dump">
<parameters>
<param name="nodeset_name" value="agent"/>
<param name="output_filename" value="agent.csv"/>
<param name="print_col_names" value="true"/>
<param name="print_row_numbers" value="true"/>
<param name="output_format" value="csv"/>
<param name="run" value="all"/>
<param name="time" value="0"/>
</parameters>
</operation>
<!-- Nodeset_dump -->
<operation name="Nodeset_dump">
<parameters>
<param name="nodeset_name" value="agentgroup"/>
<param name="output_filename" value="agentgroup.csv"/>
<param name="print_col_names" value="true"/>
<param name="print_row_numbers" value="true"/>
<param name="output_format" value="csv"/>
<param name="run" value="all"/>
<param name="time" value="0"/>
</parameters>
</operation>
<!-- Nodeset_dump -->
<operation name="Nodeset_dump">
<parameters>
<param name="nodeset_name" value="CommunicationMedium"/>
<param name="output_filename" value="CommunicationMedium.csv"/>
<param name="print_col_names" value="true"/>
<param name="print_row_numbers" value="true"/>
<param name="output_format" value="csv"/>
<param name="run" value="all"/>
<param name="time" value="0"/>
</parameters>
</operation>
<!-- Nodeset_dump -->
<operation name="Nodeset_dump">
<parameters>
<param name="nodeset_name" value="knowledge"/>
<param name="output_filename" value="knowledge.csv"/>
<param name="print_col_names" value="true"/>
</parameters>
</operation>

311
<!-- these operations help test that Construct generated node sets as the modeller expected -->

<!-- <operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="knowledgegroup" />
        <param name="output_filename" value="knowledgegroup.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<!-- <operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="binarytask" />
        <param name="output_filename" value="binarytask.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<!-- <operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="agent_type" />
        <param name="output_filename" value="agent_type.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<!-- <operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="timeperiod" />
        <param name="output_filename" value="timeperiod.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation> -->

<operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="knowledgegroup" />
        <param name="output_filename" value="knowledgegroup.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="binarytask" />
        <param name="output_filename" value="binarytask.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="agent_type" />
        <param name="output_filename" value="agent_type.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>

<operation name="Nodeset_dump">
    <parameters>
        <param name="nodeset_name" value="timeperiod" />
        <param name="output_filename" value="timeperiod.csv" />
        <param name="print_col_names" value="true" />
        <param name="print_row_numbers" value="true" />
    </parameters>
</operation>
<operation>

<!-- these operations help test that Construct read the graphs of the dynetml file correctly -->

<operation name="ReadGraphByName">

Printing the agent x agent access network before and during the attack helps modeler confirm/deny the as-evolved networks == as-designed networks -->

<parameters>
  <param name="graph_name" value="'access network'"/>
  <param name="output_filename" value="agent_access_network_attack_times.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="attacktime_output_list"/>
  <param name="operation_name" value="dump_access_network"/>
  <param name="operation_subname" value="all_time_periods"/>
  <param name="print_row_numbers" value="true"/>
  <param name="print_row_names" value="true"/>
  <param name="print_col_numbers" value="true"/>
  <param name="print_col_names" value="true"/>
  <param name="no_empty_lines" value="true"/>
  <param name="print_run_and_timeperiod" value="true"/>
</parameters>
</operation>

<operation name="ReadGraphByName">

Printing the agent x communication medium access network before and during the attack helps modeler confirm/deny the as-evolved networks == as-designed networks -->

<parameters>
  <param name="graph_name" value="'communication medium access network'"/>
  <param name="output_filename" value="agent_comms_media_access_network_attack_times.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="attacktime_output_list"/>
  <param name="operation_name" value="dump_access_network"/>
  <param name="operation_subname" value="all time periods"/>
  <param name="print_row_numbers" value="true"/>
  <param name="print_row_names" value="true"/>
  <param name="print_col_numbers" value="true"/>
  <param name="print_col_names" value="true"/>
  <param name="no_empty_lines" value="true"/>
  <param name="print_run_and_timeperiod" value="true"/>
</parameters>
</operation>
<operation name="ReadGraphByName"> <!-- Printing the agent x agent access network before and during the attack helps modeler confirm/deny the as-evolved networks == as-designed networks -->
<parameters>
    <param name="graph_name" value="'agent active timeperiod network'"/>
    <param name="output_filename" value="agent_active_timeperiod_network_attack_times.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="attacktime_output_list"/>
    <param name="operation_name" value="dump_agent_active_timeperiod_network"/>
    <param name="operation_subname" value="all_time_periods"/>
    <param name="print_row_numbers" value="true"/>
    <param name="print_row_names" value="true"/>
    <param name="print_col_numbers" value="true"/>
    <param name="print_col_names" value="true"/>
    <param name="no_empty_lines" value="true"/>
    <param name="print_run_and_timeperiod" value="true"/>
</parameters>
</operation>

<operation name="ReadGraphByName"> <!-- Printing the agent x dummy network that specifies the agent type at time 0 helps modeler confirm/deny the as-evolved networks == as-designed networks -->
<parameters>
    <param name="graph_name" value="'agent active timeperiod network'"/>
    <param name="output_filename" value="agent_active_timeperiod_network_0.csv"/>
    <param name="output_format" value="csv"/>
    <param name="run" value="all"/>
    <param name="time" value="0"/>
    <param name="operation_name" value="dump_agent_active_timeperiod_network"/>
    <param name="operation_subname" value="time_zero"/>
    <param name="print_row_numbers" value="true"/>
    <param name="print_row_names" value="true"/>
    <param name="print_col_numbers" value="true"/>
    <param name="print_col_names" value="true"/>
    <param name="no_empty_lines" value="true"/>
    <param name="print_run_and_timeperiod" value="true"/>
</parameters>
</operation>
Printing the agent x knowledge network supports exogenous to Construct analysis of knowledge based
metrics, every ten percent of the run, during attack times (+/- 1) and during brief times --
<parameters>
  <param name="graph_name" value="'knowledge network'"/>
  <param name="output_filename" value="knowledge_ten_percents_attacks_briefings.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="output_by_percentiles,attacktime_output_list,plan_briefing_time_list"/>
  <param name="operation_name" value="dump_agent_knowledge_network" />
  <param name="operation_subname" value="ten_percent_attacktime_output_list_plan_briefing_time_list" />
  <param name="print_row_numbers" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_numbers" value="true" />
  <param name="print_col_names" value="true" />
  <param name="no_empty_lines " value="true" />
  <param name="print_run_and_timeperiod" value="true" />
</parameters>
</operation>

<operation name="ReadKnowledgeDiffusionByAgentGroup"> <!-- diffusion_by_group_all -->
<parameters>
  <param name="graph_name" value="'knowledge network'"/>
  <param name="output_filename" value="diffusion_by_group_all.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="output_by_percentiles" />
  <param name="operation_name" value="dump_knowledge_diffusion_network" />
  <param name="operation_subname" value="every_ten_percent" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
</parameters>
</operation>

<operation name="KnowledgeDiffusionByIndexRange"> <!-- Print the bad plan knowledge diffusion -->
<parameters>
  <param name="graph_name" value="'knowledge network'"/>
  <param name="output_filename" value="bad_plan_k_all.csv"/>
  <param name="output_format" value="csv"/>
  <param name="run" value="all"/>
  <param name="time" value="output_by_percentiles" />
  <param name="operation_name" value="dump_knowledge_diffusion_network" />
  <param name="operation_subname" value="every_ten_percent" />
  <param name="print_run_and_timeperiod" value="true" />
  <param name="print_row_names" value="true" />
  <param name="print_col_names" value="true" />
</parameters>
</operation>
<param name="time" value="output_by_percentiles" />  
<param name="operation_name" value="dump_knowledge_diffusion_bad_plan_only" />  
<param name="operation_subname" value="every_ten_percent" />  
<param name="print_run_and_timeperiod" value="true" />  
<param name="print_row_names" value="true" />  
<param name="print_col_names" value="true" />  
<param name="index_list" value="construct::knowledgegroupvar::bad_plan_k" />  
</parameters>  
</operation>  
<operation name="KnowledgeDiffusionByIndexRange">  <!-- Print the non-bad knowledge (plan and non-plan)-->  
<parameters>  
<param name="graph_name" value="'knowledge network'"/>  
<param name="output_filename" value="non_bad_diffusion_all.csv"/>  
<param name="output_format" value="csv"/>  
<param name="run" value="all"/>  
<param name="time" value="all"/>  
<param name="operation_name" value="dump_non_bad_diffusion_all"/>  
<param name="operation_subname" value="all_time_periods"/>  
</parameters>  
</operation>  
<operation name="ReadKnowledgeDiffusion">  <!-- -->  
<parameters>  
<param name="graph_name" value="'knowledge network'"/>  
<param name="output_filename" value="diffusion_all.csv"/>  
<param name="output_format" value="csv"/>  
<param name="run" value="all"/>  
<param name="time" value="all"/>  
<param name="operation_name" value="dump_diffusion_all"/>  
<param name="operation_subname" value="all_time_periods"/>  
<param name="print_run_and_timeperiod" value="true"/>  
<param name="print_row_names" value="true"/>  
<param name="print_col_names" value="true"/>  
</parameters>  
</operation>

316
<operation name="ReadAgentsWhoDoNotInteractWithAnyone">
  <parameters>
    <param name="output_filename" value="AgentsWhoDoNotInteractWithAnyone.csv"/>
    <param name="output_format" value="csv"/>
    <param name="output_to_stdout" value="true"/>
    <param name="print_row_names" value="true"/>
    <param name="print_col_names" value="true"/>
    <param name="print_run_and_timeperiod" value="true"/>
    <param name="run" value="all"/>
    <param name="time" value="all"/>
    <param name="operation_name" value="dump_agents_who_dont_interact"/>
    <param name="operation_subname" value="all_time_periods"/>
  </parameters>
</operation>

<!-- <operation name="ReadAgentCoreTies">
  <parameters>
    <param name="output_filename" value="agent_core_ties_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="time" value="all"/>
    <param name="print_run_and_timeperiod" value="true"/>
    <param name="run" value="all"/>
    <param name="operation_name" value="dump_agents_who_dont_interact"/>
    <param name="operation_subname" value="all_time_periods"/>
  </parameters>
</operation> -->

<operation name="ActivateAltersForAgents">
  <parameters>
    <param name="output_filename" value="activateAlters_0.csv"/>
    <param name="output_format" value="csv"/>
    <param name="time" value="0"/>
    <param name="activation_network_filename" value="activateAlters_edgeList_empty.csv"/>
    <param name="symmetric_flag" value="false"/>
    <param name="load_style" value="sparse_to_dense_convert"/>
    <param name="skip_first_row" value="true"/>
    <param name="probability_of_activation" value=".5"/>
  </parameters>
</operation>

<operation name="ActivateAltersForAgents">
  <parameters>
    <param name="output_filename" value="activateAlters_0.csv"/>
    <param name="output_format" value="csv"/>
    <param name="time" value="0"/>
    <param name="activation_network_filename" value="activateAlters_edgeList_empty.csv"/>
    <param name="symmetric_flag" value="false"/>
    <param name="load_style" value="sparse_to_dense_convert"/>
    <param name="skip_first_row" value="true"/>
    <param name="probability_of_activation" value=".5"/>
  </parameters>
</operation>

<param name="activation_score_as_edge_weight" value="true"/>
</parameters>
</operation>

<!-- Used to make agents aware of a new/old set of alters with some probability at the specified time (post attack + 1) new awareness will stick. Use Case: A message to all agents of who the 'chain of command' is -->

<!-- <operation name="ActivateAltersForAgents"> -->

 ActivateAltersForAgents validated output == reasonable 28 Jan 15 -->

<!-- <operation name="ActivateAltersForAgents"> -->

 ActivateAltersForAgents validated output == reasonable 28 Jan 15 -->
<operation name="ReadAgentBeliefOfGroupKnowledgeMatrix">
  <parameters>
    <param name="output_filename" value="AvgAgentBeliefOfGroupKnowledge.csv"/>
    <param name="output_format" value="csv"/>
    <param name="time" value="all"/>
  </parameters>
</operation>

<operation name="CommunicationMediumsSent">
  <parameters>
    <param name="output_filename" value="Communications_Mediums_Sent_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="print_row_names" value="true"/>
    <param name="print_col_names" value="true"/>
    <param name="print_run_and_timeperiod" value="true"/>
    <param name="time" value="all"/>
  </parameters>
</operation>

<operation name="CommunicationMediumsReceived">
  <parameters>
    <param name="output_filename" value="Communications_Mediums_Received_all.csv"/>
    <param name="output_format" value="csv"/>
    <param name="print_row_names" value="true"/>
    <param name="print_col_names" value="true"/>
    <param name="print_run_and_timeperiod" value="true">
    <param name="time" value="all"/>
  </parameters>
</operation>

<!-- Allows experimenter to force a recalculation by ego's of their transactive memory of groups in the sim
Use Case: Can be used if some substantial change has occurred and simulator needs to tell all agents
  to reassess their understanding of the world -->
<operation name="ForceLossyIntersection">
  <parameters>
    <param name="time" value="all"/>
  </parameters>
</operation>

<!-- Prints per agent perception of groups' knowledge -->
<parameters>
  <param name="output_filename" value="activateAlters_343.csv"/>
  <param name="output_format" value="csv"/>
  <param name="time" value="construct::intvar::attack_end_time+1"/>
  <param name="activation_network_filename" value="activateAlters_edgeList.csv"/>
  <param name="symmetric_flag" value="false"/>
  <param name="load_style" value="sparse_to_dense_convert"/>
  <param name="skip_first_row" value="true"/>
  <param name="probability_of_activation" value=".5"/>
</parameters>
</operation>
<!-- availability attacks not specifically targeting key IT systems are targeting the communications mechanisms -->

<!-- Use ReadGeneralDecisionOutput to turn agent x communicationMediums on/off as a function of being during the attack time windows, and based on a probabilistic random draw being less than the modeler specified threshold -->

<operation name="ReadGeneralDecisionOutput">
<parameters>
  <param name="verbose" value="true" />
  <param name="run" value="all"/>
  <param name="time" value="attack_time_list_plus_one"/>
  <param name="output_filename" value="turn_comms_media_off_and_on.csv"/>
  <param name="output_format" value="csv"/>
  <param name="header_row" value="true"/>
  <param name="applicable_agents" value="construct::agentgroupvar::human_agent_group"/>
  <param name="decision_names" value="a_attack_web_off,a_attack_phone_off,a_attack_email_off,turn_human_agents_comms_on"/>
  <param name="a_attack_email_off" value="1"/>
  <param name="a_attack_web_off" value="if ((construct::boolvar::attack_enabled) && (timeperiod > 0) && (randomUniform(0.0,1.0) < construct::floatvar::a_attack_web_prob) && (timeperiod <= construct::intvar::attack_end_time))
   { /* setFooNetwork returns the value being set, multiple sets can occur by chaining them with a boolean AND operator to cause all to execute */

   setCommunicationMediumAccessNetwork[agent,construct::intvar::web_lvl1,0.0] &
   setCommunicationMediumAccessNetwork[agent,construct::intvar::web_lvl2,0.0]
   } else {
       1 /* non-harm else statement, since 'else' is not optional in Construct's 'if then else' statements */
  }" with="agent,verbose,timeperiod" />
  <param name="a_attack_phone_off" value="if ((construct::boolvar::attack_enabled) && (timeperiod > 0) && (randomUniform(0.0,1.0) < construct::floatvar::a_attack_phone_prob) && (timeperiod <= construct::intvar::attack_end_time)){
```xml
setCommunicationMediumAccessNetwork[agent,construct::intvar::phone_lvl1,0.0] &
setCommunicationMediumAccessNetwork[agent,construct::intvar::phone_lvl2,0.0]
} else {
  1 /* non-harm else statement */
}" with="agent,verbose,timeperiod" />
<param name="a_attack_email_off" value="
  if (construct::boolvar::attack_enabled &
  (timeperiod > 0)
  && (randomUniform(0.0,1.0) <
  construct::floatvar::a_attack_email_prob)
  && (timeperiod <=
  construct::intvar::attack_end_time)){
    setCommunicationMediumAccessNetwork[agent,construct::intvar::email_lvl1,0.0] &
    setCommunicationMediumAccessNetwork[agent,construct::intvar::email_lvl2,0.0]
  } else {
  1 /* non-harm else statement */
}" with="agent,verbose,timeperiod" />
<!-- Use ReadGeneralDecisionOutput to turn
agent x communicationMediums on after attack as
a function
of the agent being level1 or level2, or
level 2, attacks were enabled, and attacks have ended -->
<param name="turn_human_agents_comms_on"
value="
```
setCommunicationMediumAccessNetwork[$all$, construct::intvar::email_lvl2, 1.0] &
}
} else {
1 /* non-harm else statement */

" with="verbose,timeperiod" />
</parameters>
</operation>
</operations>
</construct>
Appendix 6 Lists of Tables, Figures, Equations and Acronyms

List of Tables

Table 1: Three primary sets of deliverables ................................................................. 9
Table 2: Three observations on organizational learning ............................................... 18
Table 3: Structural challenges to organizational learning .............................................. 19
Table 4: CNSSI 4009 Definitions of CIAAN ................................................................. 21
Table 5: DoD definitions of the five D’s (2006) ............................................................ 22
Table 6: Descriptive Statistics of Citations Collected for Literature Review ............... 33
Table 7: Nine (9) node metanetwork and their internode link interpretations ................ 60
Table 8: Common SNA metrics and their interpretations ............................................. 61
Table 9: Number of input files per model ................................................................. 81
Table 10: File Sizes (MB) descriptives per model/level of war – part 1 ......................... 81
Table 11: File Sizes (MB) descriptives per model/level of war – part 2 ......................... 81
Table 12: Size of D2M-Wizard generated “suggested ngrams” list and “possible acronyms” list ......................................................................................................................... 82
Table 13: Quantities of D2M-Wizard generated ngram and singleton concepts draw from the union of generated ‘concept lists’ .................................................................................. 82
Table 14: Metanetwork link descriptives for D2M cycle 0 .............................................. 83
Table 15: Metanetwork entities per ontological category for D2M cycle 0 ....................... 83
Table 16: ‘Concept list’ entities per ontological category for D2M cycle 0 ........................ 85
Table 17: ‘finalThesaurus’ entities per ontological category D2M cycle 0 ......................... 85
Table 18: Three (3) terminating conditions for D2M-process .......................................... 86
Table 19: Count per Ontological Category for each of the four final per-model thesauri (cycle 12 and higher) .............................................................................................................. 88
Table 20: Metanetwork entities per ontological category (cycle 12 and higher) ............... 88
Table 21: Metanetwork descriptives (cycle 12 and higher) ............................................ 88
Table 22: N-grams vs. Singletons, Acronyms vs. nonacronyms (cycle 12 and higher) ...... 88
Table 23: IT related agents and resources in all three generated models (cycle 12 and higher) ................................................................................................................................. 90
Table 24: Visualization options for Org x Org Models ................................................... 109
Table 25: A sample of metanetwork measures for indicators of resilience ..................... 118
Table 26: Dissertation Measures of Interest (MoI) ......................................................... 129
Table 27: Descriptive Statistics for D2M Resilience Scores .......................................... 131
Table 28: Descriptive Statistics for D2M Characteristic Path Length ............................. 131
Table 29: Descriptive Statistics for D2M Congruence, Organization, Agent Knowledge Needs .......................................................................................................................... 132
Table 30: Descriptive Statistics for D2M Congruence, Organization, Agent Knowledge Waste .......................................................................................................................... 132
Table 31: Descriptive Statistics for D2M Congruence, Organization, [Agent | IT Agent] [Resource | IT Resource] Needs, Baseline ................................................................. 133
Table 32: Descriptive Statistics for D2M Congruence, Organization, [Agent | IT Agent] [Resource | IT Resource] Waste, Baseline ................................................................. 134
Table 33: Descriptive Statistics for D2M Congruence, Organization, Task Knowledge Needs, Baseline ................................................................. 135
Table 34: Descriptive Statistics for D2M Congruence, Organization, Task Knowledge Waste ....................................................................................................................................... 136
Table 35: Descriptive Statistics for D2M Congruence, Organization, [Agent | IT Agent] [Resource | IT Resource] Waste, Baseline .............................................................................................................. 136
Table 36: Descriptive Statistics for D2M Congruence, Organization, Task [Resource | IT Resource] Waste, Baseline ............................................................................................ 137
Table 37: Descriptive Statistics for D2M Congruence, Social Technical ............................................................................................................. 138
Table 38: Descriptive Statistics for D2M Density, Clustering Coefficient ........................................................................................................... 138
Table 39: Descriptive Statistics for D2M Diffusion, Baseline ......................................................................................................................... 139
Table 40: Descriptive Statistics for D2M Fragmentation, Baseline ................................................................................................................... 140
Table 41: Descriptive Statistics for D2M Isolate Count, Baseline .................................................................................................................... 141
Table 42: Descriptive Statistics for D2M Complexity, Baseline .................................................................................................................... 141
Table 43: Descriptive statistics for D2M performance as accuracy, baseline ............................................................................................................. 142
Table 44: Descriptive Statistics for D2M Social Density, Baseline .................................................................................................................... 143
Table 45: Descriptive Statistics for D2M averageSpeed, Baseline ..................................................................................................................... 143
Table 46: Descriptive Statistics for D2M Shared Situation Awareness, Baseline ..................................................................................................... 145
Table 47: Interpreting key entity reports as a operational PDAL ......................................................................................................................... 147
Table 48: Interpreting key entity reports as strategic PDAL ............................................................................................................................. 149
Table 49: Operational Model Nodes to Remove ...................................................................................................................................... 150
Table 50: Strategic Model Nodes to Remove ...................................................................................................................................... 151
Table 51: Exogenous modifications to D2M models ................................................................................................................................... 169
Table 52: Experimental summary for D2M generated models ........................................................................................................................ 186
Table 53: 10 factor Box-Behnken design ................................................................................................................................................ 187
Table 54: Lines of code summary for Construct, pre-dissertation ................................................................................................................ 190
Table 55: Lines of code summary for Construct, post-dissertation, by Joseph, Kowalchuck and Lanham .................................................................................................................................. 190
Table 56: Lines of code added and removed during refactoring and additions ............................................................................................................. 191
Table 57: Class count changes in code base ................................................................................................................................................ 192
Table 58: Effects of random losses table ................................................................................................................................................ 200
Table 59: Rules of thumb for impacts ........................................................................................................................................................ 202
Table 60: Descriptive Statistics for D2M of Citation Titles ............................................................................................................................ 246
Table 61: Metanetwork ontological labeling heuristics ................................................................................................................................. 259
Table 62: Parameters used to in operational and strategic simulations ............................................................................................................. 278

List of Figures

Figure 1: Mission Assurance is more than Risk Management ................................................................. 5
Figure 2 Dynamic visualization of resilience for an arbitrary measure of interest (MoI) (Morgan & Lanham, 2012) ........................................................................................................................................ 6
Figure 3: Federal Communications Commission (FCC) Frequency Allocation Chart circa 2003 (US Department of Commerce, 2003) ........................................................................................................ 11
Figure 4: FCC Frequency Allocations circa 1975 (Elder, 2008) ........................................................................................................................................ 11
Figure 5: Sales growth for personal computers from 1998 to 2011 (Arthur, 2011) ................................... 12
Figure 6 Growth in installed super-computers by continent since ................................................................ 12
Figure 7 US DoD Frequency Allocation Chart circa 2010 (Defense Business Board, 2010) 13
Figure 8 Five Pillars of IA and the five D's ........................................................................................... 23
Figure 9 Intuition Based Clustering and Links Between Clusters of the Literature Corpus . 33
Figure 10 LSA 6 Topics, top 10 members/topic ................................................................. 35
Figure 11 LSA 7 Topics, top 10 members/topic ................................................................. 35
Figure 12 LSA 8 Topics, top 10 members/topic ................................................................. 35
Figure 13 LSA 9 Topics, top 10 members/topic ................................................................. 35
Figure 14 LSA 10 Topics, top 10 members/topic ............................................................... 35
Figure 15 LSA 11 Topics, top 10 members/topic ............................................................... 35
Figure 16 ORA™ generated LSA analysis of collected citations with 10 topics ............... 36
Figure 17 LDA 8 Topics, top 10 members/topic ................................................................. 38
Figure 18 LDA 9 Topics, top 10 members/topic ................................................................. 38
Figure 19 LDA 10 Topics, top 10 members/topic ............................................................... 38
Figure 20 LDA 11 Topics, top 10 members/topic ............................................................... 38
Figure 21 LDA 12 Topics, top 10 members/topic ............................................................... 38
Figure 22 LDA 13 Topics, top 10 members/topic ............................................................... 38
Figure 23 ORA™ generated LDA analysis of collected citations with 13 topics .......... 39
Figure 24 Key Entity 'Author' ......................................................................................... 42
Figure 25 Key Entity 'Journal' ......................................................................................... 42
Figure 26 Key Entity 'Publisher' ....................................................................................... 43
Figure 27 Key Entity 'Article' ......................................................................................... 43
Figure 28 Zoomed in Co-Authorship network, edges with weight < 2 hidden, zoomed in on prolific author clusters ................................................................. 44
Figure 29 Co-Authorship network, edges with weight < 3.5 hidden, pendants removed, not zoomed in ................................................................. 44
Figure 30 Zoomed in Co-Authorship network, edges with weight < 3.5 hidden, with pendants removed, zoomed in on prolific authors ......................................................... 44
Figure 31 Zoomed in Co-Authorship network, edges with weight < 3.5 hidden, with pendants remaining, zoomed in on prolific authors ................................................................. 45
Figure 32 Co-citation network of Article x Article, no filtering ........................................ 45
Figure 33 Co-citation network of Article x Book, no filtering ............................................ 46
Figure 34 Four-node metanetwork ..................................................................................... 61
Figure 35 Stylized Dissertation Workflow .......................................................................... 70
Figure 36 Dissertation Workflow Data to Model (D2M) .................................................. 72
Figure 37 Data to Model (D2M) Wizard applied to any input corpus ............................ 74
Figure 38 D2M refinement applied to DoD input corpus .................................................. 75
Figure 39 Simplified DoD Hierarchy--Strategic to Operational ..................................... 77
Figure 40 Simplified figure of USG strategic level organizations .................................. 78
Figure 41 Simplified figure of COCOM and USAF operational level organizations ...... 79
Figure 42 USAF Doctrinal Air Operations Center (AOC) Organizational Structure ...... 80
Figure 43 USAF AOC as a text mined model of links and nodes .................................... 80
Figure 44 Size of D2M-Wizard generated ngram list and possible acronym list .......... 82
Figure 45 Quantities of D2M-Wizard generated ngram and singleton concepts draw from the union of generated 'concept lists' ........................................... 83
Figure 46 Recurring Top Ranked Agents (top 3), Operational Model ......................... 91
Figure 47 Recurring Top Ranked Agents (top 20), Operational Model ....................... 92
Figure 48 Recurring Top Ranked Human Agents (top 3), Operation Model .................. 92
Figure 49 Recurring Top Ranked Human Agents (top 20), Operational Model .......... 93
Figure 50 Recurring Top Ranked IT agents (top 3), Operational Model ........................................ 94
Figure 51 Recurring Top Ranked IT agents (top 20), Operational Model .................................. 94
Figure 52 Recurring Top Ranked Organizations (top 3), Operation Model ................................. 95
Figure 53 Recurring Top Ranked Organizations (top 20), Operational Model ............................ 95
Figure 54 Recurring Top Ranked Resources (top 3), Operational Model .................................. 96
Figure 55 Recurring Top Ranked Resources (top 20), Operational Model ................................. 96
Figure 56 Recurring Top Ranked Non-IT resources (top 3), Operational Model ......................... 97
Figure 57 Recurring Top Ranked Non-IT resources (top 20), Operational Model ....................... 98
Figure 58 Recurring Top Ranked IT resources (top 3), Operational Model ............................... 98
Figure 59 Recurring Top Ranked IT resources (top 20), Operational Model ............................. 99
Figure 60 Recurring Top Ranked Agents (top 3), Strategic Model ............................................. 100
Figure 61 Recurring Top Ranked Agents (top 20), Strategic Model .......................................... 101
Figure 62 Recurring Top Ranked Human Agents (top 3), Strategic Model ............................... 102
Figure 63 Recurring Top Ranked Human Agents (top 20), Strategic Model ............................... 102
Figure 64 Recurring Top Ranked IT agents (top 3), Strategic Model ......................................... 103
Figure 65 Recurring Top Ranked IT agents (top 20), Strategic Model ........................................ 103
Figure 66 Recurring Top Ranked Organizations (top 3), Strategic Model ................................. 104
Figure 67 Recurring Top Ranked Organizations (top 20), Strategic Model ............................... 105
Figure 68 Recurring Top Ranked Resources (top 3), Strategic Model ........................................ 105
Figure 69 Recurring Top Ranked Resources (top 20), Strategic Model .................................... 106
Figure 70 Recurring Top Ranked Non-IT resources (top 3), Strategic Model .............................. 107
Figure 71 Recurring Top Ranked Non-IT resources (top 20), Strategic Model ............................. 107
Figure 72 Recurring Top Ranked IT resources (top 3), Strategic Model ...................................... 108
Figure 73 Recurring Top Ranked IT resources (top 20), Strategic Model ................................... 108
Figure 74 Node color legend for Operational Organization x Organization visualizations ......... 110
Figure 75 Operational Org x Org, no filtering by link weight ...................................................... 110
Figure 76 Operational Org x Org, filtering by level of warfare != blank (the level is unambiguously within scope, exogenously determined by researcher) .................................... 110
Figure 77 Operational Org x Org, filtering by link weight >= 15 ............................................. 110
Figure 78 Operational Org x Org, filtering by link weight >= 35 ............................................... 111
Figure 79 Node color legend for Strategic Organization x Organization visualizations ......... 112
Figure 80 Strategic Org x Org, no filtering by link weight ............................................................ 112
Figure 81 Strategic Org x Org, filtering by link weight >= 15 ..................................................... 112
Figure 82 Strategic Org x Org, filtered by model scope ................................................................. 112
Figure 83 Strategic Org x Org, filtering by link weight >= 35 ..................................................... 112
Figure 84 Dissertation workflow static analysis prior to augmentation for agent based modeling .................................................................................................................................. 115
Figure 85 Dynamic visualization of resilience for an arbitrary measure of interest (MoI) (Morgan & Lanham, 2012) .......................................................... 115
Figure 86 2D projection of 3D rendering of two access indices .................................................. 122
Figure 87 Sigmoid function of Knowledge + Resource Needs Component, low input values best .................................................................................................................. 123
Figure 88 Sigmoid function of Knowledge + Resource Waste Component, high input values best .............................................................................................................. 125
Figure 89 2D rendering of resilience score, as function of access indices, wastes, and needs .................................................................................................................................. 127
Figure 90 Surface mapping of interaction between a single waste and a single needs/access value .............................................................................................................................. 127
Figure 91 3D surface rendering of theoretical resilience scores, as function of access indices, wastes, and needs ........................................................................................................ 128
Figure 92 congruenceOrg[Agent | IT Agent] [Resource | IT Resource]Needs score .................. 133
Figure 93 congruenceOrg[Agent | IT Agent][Resource | IT Resource] Waste, Baseline .... 133
Figure 94 congruenceOrgTaskKnowledgeNeeds, Baseline ............................................ 135
Figure 95 congruenceOrgTaskKnowledgeWaste, Baseline ............................................. 135
Figure 96 congruenceOrgTaskResource Needs, Baseline ............................................. 137
Figure 97 congruenceOrgTaskResource Waste, Baseline ............................................. 137
Figure 98 clusteringCoefficient Needs, Baseline .......................................................... 139
Figure 99 diffusion [[it]agent | itresource], Baseline ....................................................... 139
Figure 100 Fragmentation, Baseline .............................................................................. 140
Figure 101 isolateCount [[IT]Agent|Resource], Baseline ................................................. 140
Figure 102 performanceAsAccuracy, Baseline ............................................................... 142
Figure 103 Social Density, Baseline .............................................................................. 143
Figure 104 averageSpeed, Baseline .............................................................................. 144
Figure 105 Shared Situation Awareness (Agent and IT Agent), Baseline ......................... 144
Figure 106 Resilience Score for entropic and targeted deletions ....................................... 152
Figure 107 Changes in Characteristic Path Length of IT agents for entropic and targeted deletions .................................................................................................................... 153
Figure 108 Changes in Communication Speed of IT agents for entropic and targeted deletions ....................................................................................................................... 153
Figure 109 Changes in Clustering Coefficient of IT agents for entropic and targeted deletions ....................................................................................................................... 153
Figure 110 Changes in diffusion of IT agents for entropic and targeted deletions ............... 155
Figure 111 Changes in Fragmentation of IT agents for entropic and targeted deletions .... 155
Figure 112 Change in isolate count of IT agents for entropic and targeted deletions ....... 156
Figure 113 Overall changes in complexity ..................................................................... 157
Figure 114 Change in social density of IT agents ........................................................... 157
Figure 115 Changes in Performance as Accuracy of Agents ........................................... 158
Figure 116 Changes to Performance as Accuracy of Roles ............................................. 159
Figure 117 Changes to performance as accuracy of IT agents ........................................ 160
Figure 118 Dissertation workflow augmentation of models for use in ABM ...................... 168
Figure 119 Knowledge x knowledgegroup network ..................................................... 171
Figure 120 Agent x Communications Medium (Operational) ......................................... 176
Figure 121 Shared planning knowledge .......................................................................... 182
Figure 122 Graphical rendering of experimental setup with factor tree and Box-Behnken leaves ..................................................................................................................... 186
Figure 123 Dissertation workflow executing simulations of models ............................... 189
Figure 124 Baseline ‘plan’ diffusion for operational model .......................................... 194
Figure 125 Baseline ‘plan’ diffusion for strategic model .................................................... 195
Figure 126 Baseline performance as accuracy for operational model ......................... 195
Figure 127 Baseline performance as accuracy for strategic model ................................. 195
Figure 128 Strategic model linear effects for single-vector attack conditions ................. 196
Figure 129 Strategic model non-linear effects for multi-vector attack conditions ............ 196
Figure 130 Strategic model with newcomer training modeled as a reduction in transactive memory error rates ........................................................................................................ 197
Figure 131 Strategic model with post-event diffusion better with spares than in the baseline condition. ...................................................................................................................... 197
Figure 132 Operational model linear effects for single-vector attack conditions .......................................................... 197
Figure 133 Operational model non-linear effects for multi-vector attack conditions .......... 197
Figure 134 Operational model with newcomer training modeled as a reduction in transactive memory error rates ........................................................................................................ 198
Figure 135 Operational model with post-event diffusion better with spares than in the baseline condition. ...................................................................................................................... 198
Figure 136 USAF Visual Depiction of Mission Assurance (Elder, 2008) .......................................................... 232
Figure 137 Dynamic visualization of resilience for an arbitrary measure of interest (MoI)(Morgan & Lanham, 2012) ........................................................................................................ 234
Figure 138 Dynamic visualization of resilience for an arbitrary measure of organization (MoO)(Morgan & Lanham, 2012) ........................................................................................................ 236
Figure 139 Data-to-Model (D2M) User Interface of AutoMap .......................................................................................... 245
Figure 140 Concept x TFIDF .......................................................................................................................................................... 246
Figure 141 TFIDF x Cumulative Percentage of $\Sigma$ TFIDF ........................................................................................................ 247
Figure 142 Directory structure for virtual experiments ........................................................................................................ 265
Figure 143 Directory structure for construct within virtual experiment directory structure .......................................................................................................................... 265
Figure 144 Snapshot of params_template.xls, Columns A-H .......................................................................................... 267
Figure 145 Snapshot params_templat.xls, Columns E-J ........................................................................................................ 268
Figure 146 Snapshot of experiment_config_file.xls ........................................................................................................ 270
Figure 147 Directory structure for construct runs ........................................................................................................ 272
Figure 148 Eclipse’s Run configurations menu item ........................................................................................................ 273
Figure 149 Eclipse run configuration for NetworkDataAggregator – main tab ........................................................................ 274
Figure 150 Eclipse run configuration for NetworkDataAggregator – arguments tab ........................................................................ 275

List of Equations

Equation 1 Risk as a function of the probability of occurrence and the forecasted impact... 23
Equation 2 Risk as a function of three variables: threat nature, vulnerability nature, and asset value.......................................................... 23
Equation 3 Node set definition in set notation ........................................................................................................ 40
Equation 4 Edge set definition in set notation ........................................................................................................ 40
Equation 5 Measures set definition in set notation ........................................................................................................ 40
Equation 6 A measure’s output definition in set notation ........................................................................................................ 40
Equation 7 A set of maximum values from a measure’s output in set notation ........................................................................ 40
Equation 8 A set of node identifiers corresponding to maximum values from a single measure in set notation ........................................................................................................ 40
Equation 9 A set of measures’ results as sets of node identifiers in set notation ........................................................................ 41
Equation 10 Calculating the frequency of occurrence a node is in the maximum value set of all relevant measures ........................................................................................................ 41
Equation 11 A set of maximum frequency of occurrence values in set notation ........................................................................ 41
Equation 12 A set of node identifiers corresponding to maximum frequency of occurrence values in set notation ........................................................................................................ 41
Equation 13 Resilience as a function of the magnitude of transformation, the frequency of
transformation, time, expense, and emotional energy ........................................................ 55
Equation 14 Structural resilience as a new metanetwork calculation ..................................... 119
Equation 15 Access index as reflection of criticality through near isolation (Kathleen M.
Carley, Juergen Pfeffer, et al., 2012) .............................................................................. 120
Equation 16 Normalized summation of a model’s knowledge access index, agents aggregated ................................................................. 120
Equation 17 Knowledge access component sigmoid, right shifted six values, in 12 bins.... 120
Equation 18 Normalized summation of a model’s knowledge access index, agents
disaggregated ..................................................................................................................... 121
Equation 19 Knowledge access component sigmoid, right shifted six values, in 12 bins,
agents disaggregated ....................................................................................................... 121
Equation 20 Normalized summation of a model’s task access index, agents disaggregated 121
Equation 21 Normalized summation of a model’s resource and IT resource access index,
agents disaggregated ...................................................................................................... 121
Equation 22 Access Index Component, adjusted for disaggregation of Agent and Resource
node sets ............................................................................................................................ 121
Equation 23 Tasks with needed knowledge via assigned agents (Kathleen M. Carley, Juergen
Pfeffer, et al., 2012) ........................................................................................................ 123
Equation 24 Percentage of knowledge not provided by agents assigned to tasks (Knowledge
Needs) (Kathleen M. Carley, Juergen Pfeffer, et al., 2012) .............................................. 123
Equation 25 Knowledge needs, right shifted 6 values, in 12 bins ......................................... 123
Equation 26 Needs Component as sum of two sigmoid needs functions, right shifted 6 values,
in 12 bins ......................................................................................................................... 123
Equation 27 congruenceOrgTaskKnowledgeNeeds with disaggregated agents and IT agents
(Kathleen M. Carley, Juergen Pfeffer, et al., 2012) ........................................................... 123
Equation 28 Tasks with needed resources via assigned agents (Kathleen M. Carley, Juergen
Pfeffer, et al., 2012) ........................................................................................................ 124
Equation 29 Percentage of resources not provided by agents assigned to tasks (Kathleen M.
Carley, Juergen Pfeffer, et al., 2012) ............................................................................. 124
Equation 30 Resource needs, right shifted 6 values, in 12 bins ............................................ 124
Equation 31 congruenceOrgTaskResourceNeeds with disaggregated agents and IT agents
(Kathleen M. Carley, Juergen Pfeffer, et al., 2012) ........................................................... 124
Equation 32 Percentage of knowledge not used for tasks assigned to agents (Kathleen M.
Carley, Juergen Pfeffer, et al., 2012) ............................................................................. 125
Equation 33 Knowledge waste, right shifted 6 values, in 12 bins ........................................ 125
Equation 34 congruenceOrgTaskKnowledgeWaste with disaggregated agents and IT agents
(Kathleen M. Carley, Juergen Pfeffer, et al., 2012) ........................................................... 125
Equation 35 Percentage of resources not used for tasks assigned to agents (Kathleen M.
Carley, Juergen Pfeffer, et al., 2012) ............................................................................. 125
Equation 36 Resource ‘Waste,’ right shifted 6 values, in 12 bins .......................................... 126
Equation 37 congruenceOrgTaskResourceNeeds with disaggregated agents and IT agents
(Kathleen M. Carley, Juergen Pfeffer, et al., 2012) ........................................................... 126
Equation 38 Waste Component as sum of two sigmoid waste functions, right shifted 6 values,
in 12 bins ......................................................................................................................... 126
Equation 39 Law of Cosines to calculate distances between two points on a sphere ......... 182
Equation 40 Generating an agent x location network (count of shared organization) ........ 183
Equation 41 Generating an agent x location network (sum of distances between ego
instances) ....................................................................................................................... 183
Equation 42 Generating an agent x agent network (count of shared locations) ........... 183
Equation 43 Generating an agent x agent (sum of distances between egos and alters) ...... 183
Equation 44 Generating average distance between ego and alter agents ..................... 184
Equation 45 Generating an agent x agent physical proximity network for use by Construct,
scale [1.0,0.0,0] ............................................................................................................ 184
Equation 46 Naive experimental summary ..................................................................... 187
Equation 47 Term Frequency for Concept x ................................................................. 245
Equation 48 Inverse Document Frequency for Term x in Corpus .................................. 246
Equation 49 Term Frequency x Inverse Document Frequency (TFIDF) ......................... 246
**Acronyms**

- **CASOS**  Center for Computational Analysis of Social and Organizational Systems
- **CNSS**  Committee of National Security Systems
- **DNA**  dynamic network analysis
- **EECS**  Electrical Engineering and Computer Science
- **IA**  Information Assurance (IA)
- **IT**  information technology
- **MoE**  measures of effectiveness
- **MoP**  measures of performance
- **SNA**  social network analysis
- **USMA**  United States Military Academy
- **USAF**  United States Air Force
operations  
military  4, 78, 100, 174, 231
orders  
cyber related  79
organizations  
  high reliability  10
Perl  74
Pfeffer, Jürgen  iv
power-law  153
random outages  146, 153
regular expression  74
rehearsals  49, 185, 196, 236
organizational  1, 6, 9, 10, 14, 18, 37, 65, 66, 67, 69, 113, 117, 159, 209, 232, 239
resiliency  v, 9, 139, 162, 265
resilient  1, 17, 23, 29, 31, 52, 53, 54, 56, 57, 68, 86, 126, 153, 232, 239
risk  
  reduction  4, 49
SCADA  9, 15, 28
SCM  10, 50, 51, 52, 63
security level  3
single point of failure  See SPOF
SNA  1, 330
social network analysis  1, 39, 114, 129, 160, 330
Super Storm Sandy  8, 14, 27
supervisory control and data acquisition  9
supply chain  8, 10, 36, 52, 63, 67
text mining  v, 239
thesaurus  75
  acronym  75
  case sensitive  75
  dissertation  75
  model-specific  75
threats  
  cyber  8, 14, 25
united states military academy  330
USAF  4, 19, 78, 79, 80, 86, 94, 173, 231, 232, 330
USMA  iv, 330
vectors  
  attack  3
vulnerabilities  
  structural  v, 1
Watson, Tom  11
Wei, Wei  iv
White House  13
Wizard  D2M  73, 76
work product  75