NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFICIENCY VS. SECURITY: INFORMATION TECHNOLOGY CONSOLIDATIONS—RESILIENCE, COMPLEXITY, AND MONOCULTURE

by

Jennifer L. Ricker

March 2018

Thesis Co-Advisors: Ted G. Lewis
Scott Jasper

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE EFFICIENCY VS. SECURITY: INFORMATION TECHNOLOGY CONSOLIDATIONS—RESILIENCE, COMPLEXITY, AND MONOCULTURE		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jennifer L. Ricker			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Governmental organizations commonly seek to cut costs and increase efficiency through consolidation and standardization of information technology (IT) infrastructure. This may result in vulnerabilities not typically considered by policymakers, due to concentration and homogenization of critical assets, elimination of redundancy and surge capacity, and tightly coupled systems. This thesis reviewed the potential vulnerabilities that may exist in consolidated IT systems due to the effects of complexity, self-organized criticality, and monoculture, and shows that efficient systems carry inherent vulnerabilities. Because we cannot mitigate every possible threat, hazard, or vulnerability, IT professionals should focus on system resilience. Resilience of a system is counter-proportional to the product of vulnerability and spectral radius; therefore, any increase in vulnerability, spectral radius, or both decreases resilience. A reduction in overall vulnerability can compensate for increased self-organization and other losses of resilience through a variety of recommended actions. Many of those actions come with a cost—organizations will have to determine the tradeoffs they are willing to make between efficiency and security.

14. SUBJECT TERMS complexity, resilience, monoculture, efficiency, security, self-organization, IT consolidation			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

EFFICIENCY VS. SECURITY: INFORMATION TECHNOLOGY CONSOLIDATIONS—RESILIENCE, COMPLEXITY, AND MONOCULTURE

Jennifer L. Ricker
Acting Director, Illinois Emergency Management Agency, Springfield, IL
B.A., University of Missouri–Columbia, 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2018**

Approved by: Ted G. Lewis, Ph.D.
Co-Advisor

Scott Jasper, CAPT, USN (Ret)
Co-Advisor

Erik Dahl, Ph.D.
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Governmental organizations commonly seek to cut costs and increase efficiency through consolidation and standardization of information technology (IT) infrastructure. This may result in vulnerabilities not typically considered by policymakers, due to concentration and homogenization of critical assets, elimination of redundancy and surge capacity, and tightly coupled systems. This thesis reviewed the potential vulnerabilities that may exist in consolidated IT systems due to the effects of complexity, self-organized criticality, and monoculture, and shows that efficient systems carry inherent vulnerabilities. Because we cannot mitigate every possible threat, hazard, or vulnerability, IT professionals should focus on system resilience. Resilience of a system is counter-proportional to the product of vulnerability and spectral radius; therefore, any increase in vulnerability, spectral radius, or both decreases resilience. A reduction in overall vulnerability can compensate for increased self-organization and other losses of resilience through a variety of recommended actions. Many of those actions come with a cost—organizations will have to determine the tradeoffs they are willing to make between efficiency and security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. INFORMATION TECHNOLOGY....2
B. INFORMATION TECHNOLOGY—CRITICAL INFRASTRUCTURE....3
C. ORGANIZATIONAL CONSOLIDATIONS OF INFORMATION TECHNOLOGY....5
D. PROBLEM STATEMENT AND RESEARCH QUESTION....7
E. RESEARCH DESIGN....8

II. THEORIES AND CONCEPTS....9
A. LITERATURE REVIEW....9
B. INFORMATION TECHNOLOGY CONSOLIDATIONS....11
1. AT&T Long-Distance Network Collapse....13
2. Office of Personnel Management Data Breach....14
3. Illinois State Board of Elections Attack....16
C. COMPLEXITY....17
D. MONOCULTURE....21
E. RESILIENCE AND EFFICIENCY....22

III. ILLINOIS IT TRANSFORMATION....25
A. CURRENT STATE....25
B. FUTURE STATE PLAN....27

IV. ANALYSIS....31
A. QUANTIFYING SELF-ORGANIZATION....31
B. STATE OF ILLINOIS....33
C. CONSOLIDATION IN THE CLOUD....37

V. CONCLUSION AND RECOMMENDATIONS....41
A. CONCLUSION....41
B. RECOMMENDATIONS....41

LIST OF REFERENCES....47

INITIAL DISTRIBUTION LIST....51

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Network Types....20

Figure 2. Enterprise Operating Model....28

Figure 3. State of Illinois Network circa 2015....35

Figure 4. Illinois Future State Representation....36

Figure 5. Network Resiliency....37

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Consolidation Strategies and Benefits 6

Table 2. Features of Emergence 18

Table 3. Vulnerability 33

Table 4. Spectral Radius 33

Table 5. Cloud-Specific Vulnerabilities 38

Table 6. Typical Enterprise System Vulnerabilities and Countermeasures 43

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CMS	Department of Central Management Service (state of Illinois)
DHS	Department of Homeland Security
DoIT	Department of Innovation and Technology (state of Illinois)
IT	information technology
ITSSP	Information Technology Sector-Specific Plan Annex
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management
SOC	self-organized criticality

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Governments, like other organizations dealing with budgetary pressures, typically search for ways to increase efficiency and effectiveness. One common way of cutting costs and increasing efficiency is to consolidate information technology (IT) systems. IT is a critical component of the nation's infrastructure, economy, and government operations; the U.S. Department of Homeland Security designated the IT sector as one of the seventeen critical infrastructure sectors.[1] The state of Illinois is currently undergoing a consolidation of all state agency IT systems with the goal of a highly centralized and optimized monoculture environment.[2] However, policymakers typically do not consider whether concentration and homogenization of critical assets, elimination of redundancy and surge capacity, and tight coupling may result in other system vulnerabilities.

This thesis considers theories and research that indicate highly connected, hyper-efficient systems contain the seeds of their own failures.[3] The focus is specifically on the potential vulnerabilities that exist in consolidated IT systems due to the effects of complexity, self-organized criticality (SOC), and monoculture, as well as the impact of those effects on system resilience. The thesis includes a high-level analysis of current and potential weaknesses that result from complexity and hardware and software monocultures, as well as the potential impact of heavy usage of cloud computing. The thesis also includes a representative analysis of the consolidation in Illinois that began in 2015.

Through quantification of self-organization, we determine system vulnerability and resilience in order to help understand how to mitigate the identified vulnerabilities. The two main drivers of self-organizing networks—percolation and preferential

---

[1] "Information Technology Sector," Department of Homeland Security, accessed March 26, 2017, https://www.dhs.gov/information-technology-sector.

[2] Illinois Office of the Secretary of State, *Executive Order Consolidating Multiple Information Technology Functions into a Single Department of Innovation and Technology*, Illinois Executive Order 2016-01 (Springfield, IL: Senate of Illinois Executive Department, 2016), https://www2.illinois.gov/Documents/ExecOrders/2016/ExecutiveOrder2016-01.pdf.

[3] Ted G. Lewis, *Bak's Sandpile: Strategies for a Catastrophic World*, Kindle ed. (Williams, CA: Agile Press, 2011), loc. 32.

attachment—are combined into a single quantity called spectral radius. As SOC increases, so does spectral radius. Vulnerability is defined as the probability of collapse when an asset such as a hardware or software component is stressed. System vulnerability relates to stresses such as monoculture, surge capacity, and weakness in nodes or links. Higher values of vulnerability mean lower values of resilience, also. When we combine vulnerability (v) and spectral radius (r) into a product (vr), we combine the effects of SOC with the effects of stresses into a single measure of fragility. The system's structure determines how resilient the system is, not simply each component's weakness.

The thesis concludes that vulnerability increases with consolidation and optimization, thereby reducing system resilience. While high-consequence, extreme events happen less frequently than smaller-consequence events, with increased vr the big events will be even more damaging.[4] The objective of resilient system design is to reduce v, r, or both. Examples of both pre-consolidation and anticipated post-consolidation portions of the Illinois network were analyzed for resilience by simulating cascades initiated by failure of a randomly chosen node. This analysis demonstrated an increasingly self-organized and fragile system.

The research concludes that when consolidating and centralizing to save money, system designers and administrators need to take special precautions to offset the downside of centralization and standardization with extra vulnerability-reducing precautions. This typically means that hardware and software systems and communication networks must be hardened even more against accidental and deliberate attacks. That is, vulnerability must be reduced to compensate for the increase in self-organization. Mathematically, this means vulnerability (v) must be reduced to offset spectral radius (r).

Because vulnerability is counter-proportional to resilience, the thesis recommends reducing overall vulnerability in order to compensate for increased self-organization and loss of resilience. Vulnerabilities in an enterprise system can be the result of a variety of issues, including design flaws in software or hardware, or organizational policy

[4] Lewis, loc. 872.

weaknesses. Examples of typical vulnerabilities and countermeasures are provided. Recommendations regarding identified areas of vulnerability in cloud computing as well as suggestions for mitigating SOC and monoculture are also provided. Although we cannot mitigate for every possible threat, hazard, or vulnerability, organizations should focus on actions that will increase resilience, several of which are proposed. There will be a cost to many of the proposed solutions, but they are flexible enough to allow organizations to determine the tradeoffs they are willing to make between efficiency and security.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Foremost, I would like to thank the brilliant Dr. Ted G. Lewis, who blew my mind during the first IR with discussion of complexity and self-organized criticality. I am grateful for your guidance, patience, and genius. Thank you to Scott Jasper for your encouragement and feedback and, most of all, your insistence that I would be able to finish this!

Thanks to the other two legs of the once "three-legged-stool"—friends and colleagues James K. Joseph and Joseph G. Klinger—for encouraging and supporting me in this endeavor. Thank you to Illinois CIO and Secretary of DoIT, Kirk Lonbom, and his staff for their assistance with this research. I hope you find something valuable here as we continue Illinois' IT transformation. Thank you to my staff at IEMA for picking up the slack during my absences. Having such great staff made it easy to focus on school when I needed to.

To cohort 1605/1606 (1611), thanks for the laughter, encouragement, and friendship. And especially to the extended Pack of close friends made in this cohort—I seriously could not have survived without you. Your smiles, wicked smahts, fluent sarcasm, and poetic song have made it all worth it. Thanks to "The Patio" for keeping me sane.

Finally, to my family: There are not enough words to express how thankful I am for your support. To my husband, Sean, who took care of pretty much everything without complaint for the last eighteen months. To my son, Cole, who has always been mature beyond his years, for stepping up and being responsible and understanding. To my mother, Cheryl, for being an exceptional role model throughout my life who taught me the value of education and the drive to pursue what I want. To my father, Cliff, for all of the love and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Information technology (IT) is a critical component of the nation's infrastructure, economy, and government operations. The U.S. Department of Homeland Security (DHS) has designated the IT sector as one of the seventeen critical infrastructure sectors.[1] Each of the other critical infrastructure sectors also rely on the IT sector's products, making efforts to ensure the security and resilience of the sector even more important.[2]

Governments, like other organizations dealing with budgetary pressures, typically search for ways to increase efficiency and effectiveness. One common way of cutting costs and increasing efficiency is to consolidate IT systems. Illinois is currently undergoing a consolidation of all state agency IT systems with the goal of creating a highly centralized and optimized environment.[3] The federal government, as well as many other states are attempting—or have attempted—consolidations for similar reasons.[4] It makes sense to reduce costs and it seems wasteful to have redundant systems with excess capacity. State and federal budgets have faced considerable pressure for decades, so reducing spending that could otherwise be used for something else or to reduce taxes has long been a priority of political leaders.

Generally not considered, however, is whether concentration and homogenization of critical assets, elimination of redundancy and surge capacity, and extreme connectivity results in other system vulnerabilities. Theories and research developed over the last three

---

[1] "Information Technology Sector," Department of Homeland Security, accessed March 26, 2017, https://www.dhs.gov/information-technology-sector.

[2] Department of Homeland Security (DHS), *Information Technology Sector-Specific Plan (ITSSP): An Annex to the NIPP 2013* (Washington, DC: Department of Homeland Security, 2016), www.dhs.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf.

[3] Illinois Office of the Secretary of State, *Executive Order Consolidating Multiple Information Technology Functions into a Single Department of Innovation and Technology*, Illinois Executive Order 2016-01 (Springfield, IL: Senate of Illinois Executive Department, 2016), https://www2.illinois.gov/Documents/ExecOrders/2016/ExecutiveOrder2016-01.pdf.

[4] "Introducing the IT Shared Services Strategy," White House, May 2, 2012, https://obamawhitehouse.archives.gov/blog/2012/05/02/introducing-it-shared-services-strategy; Madeleine Bayard and Erin Lee, "Review of State Information Technology Consolidation Efforts" (issue brief, NGA Center for Best Practices, 2005), https://www.nga.org/files/live/sites/NGA/files/pdf/0512Consolidationissuebrief.pdf.

decades are proving that the most efficient systems can be the most fragile, susceptible to failure from slight perturbations that can cascade through the system.[5] The more tightly coupled the system, the more potential exists for catastrophic failure.

Making the assumption that we cannot mitigate every possible threat, hazard, or vulnerability, we should focus on resilience. According to DHS, resilience means the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[6] But efficient systems carry inherent vulnerabilities; how do we balance efficiency and resiliency to ensure system security?

A. INFORMATION TECHNOLOGY

To provide better understanding and define specifically what is meant when using the phrase "information technology" or "IT," this thesis uses the National Institute of Standards and Technology (NIST) definition. NIST defines IT as follows:

> Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency …. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.[7]

Additionally, "hardware" refers to physical components of a system. This includes personal computers and devices but, as part of network infrastructure, hardware also includes items such as routers and switches. Software, on the other hand, refers to programs and instructions given to the hardware to perform tasks. "Network" is defined for this thesis as interconnected components that include both hardware and software.

---

[5] Per Bak, Chao Tang, and Kurt Wiesenfeld, "Self-Organized Criticality: An Explanation of 1/f Noise," *Physical Review Letters* 59, no. 4 (July 27, 1987): 381–84.

[6] DHS Security Risk Steering Committee, *DHS Risk Lexicon: 2010 Edition* (Washington, DC: Department of Homeland Security, 2010), https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

[7] Richard Kissel (Ed.), *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, (Gaithersburg, MD: NIST, 2013), 100, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

B. INFORMATION TECHNOLOGY—CRITICAL INFRASTRUCTURE

Certain national infrastructure components have been deemed "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[8] Presidential Policy Directive 21 (PPD 21) establishes a national policy to ensure unity of effort in order to protect the nation's critical infrastructure.[9] Information technology now underlies all of the other sectors, making it vitally important to reduce risks and ensure system resiliency. The 2014 Quadrennial Defense Review notes that potential adversaries are probing our critical infrastructure, which could result in significant damage to the country and economy.[10]

The IT sector includes businesses and individuals that provide IT hardware, software, systems, and services.[11] It is also closely linked with, but separate from, the communications sector, which is characterized by physical and electronic means of communication. The communications sector "has evolved from a largely mechanical, circuit-switched network carrying voice telephone calls … to a highly complex integrated system of computer-controlled, packet-based networks carrying voice, data, and video."[12] The IT sector continues to rapidly evolve as well. Trends in the sector include increased use of cloud computing, deployment of internet-connected devices known as the Internet of Things, and an overall increase in operational complexity.[13] As described in the Information Technology Sector-Specific Plan Annex (ITSSP) to the National Infrastructure Protection Plan, "unlike some other Sectors, the IT Sector is a functions-

---

[8] "Critical Infrastructure Sectors," DHS, last updated July 11, 2017, https://www.dhs.gov/critical-infrastructure-sectors.

[9] President of the United States, *Critical Infrastructure Security and Resilience*, PPD-21 (Washington, DC, 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[10] Department of Defense, *2014 Quadrennial Defense Review* (Washington, DC: Department of Defense, 2014), 7, https://www.defense.gov/Portals/1/features/defenseReviews/QDR/2014_Quadrennial_Defense_Review.pdf.

[11] DHS, *ITSSP*, iii.

[12] DHS, 4.

[13] DHS, 3.

based Sector that comprises not only physical assets, but also virtual systems and networks that enable key capabilities and services in both the public and private sectors."[14] So physical assets as well as virtual ones need to be hardened and protected.

Physically hardening the location of IT hardware is relatively straightforward. We can keep servers, switches, and computers behind locked doors and secured facilities. We can also harden facilities against naturally occurring events, such as tornadoes or earthquakes. But the virtual aspect, the network connections that open an enterprise to the rest of the world through the internet, can become complicated, particularly when they attempt to balance an organization's security needs with the ease of use demanded by the end user. Additionally, the increasing use of cloud services and storage adds new complexity for an organization in ensuring both physical and cyber security are maintained by the entity providing the service. As noted by DHS, "cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks."[15]

The risks described in the ITSSP, however, are mainly related to deliberate, manmade attacks as well as an unintentional, manmade incidents and natural disasters. The document does not contemplate or address potential vulnerabilities from the structure and behavior of a system itself.

While critical infrastructure systems may appear simple, they typically evolve from disparate collections of assets toward a more connected, efficient structure and greater levels of self-organization.[16] This self-organization emerges over time as a result of centralization, reduction in surge capacity and redundancy, and development of a monoculture. For instance, the goal of optimizing systems to be as efficient as possible,

---

[14] DHS, iii.

15 "Cybersecurity Overview," DHS, accessed November 18, 2017 https://www.dhs.gov/cybersecurity-overview.

[16] Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* 2nd ed. (Hoboken, NJ: John Wiley & Sons, 2015), 64.

particularly within a consolidated information technology environment, is more of a continuous evolution than a structure that becomes designed as more and more pieces are joined together. Dr. Ted Lewis states that "self-organized systems are typically nonredundant, nonsurge capable single-point-of-failure systems with bottlenecks, overly concentrated assets, and inadequate backup capacity."[17] Yet this type of vulnerability is not addressed in national critical infrastructure planning.

C. ORGANIZATIONAL CONSOLIDATIONS OF INFORMATION TECHNOLOGY

Many public-sector organizations, including Illinois state agencies, have historically operated independent IT operations in each agency or department, each with its own infrastructure, often resulting in redundant systems and excess capacity. This independence allowed agencies to build IT infrastructure and applications that were customized and responsive to agency needs. When there are no overarching IT strategies or standardized requirements across the enterprise, infrastructure, networks, and applications are built on diverse hardware and software platforms.

Government organizations, like most others, are faced with mounting pressure to reduce costs and deliver better services to citizens. As a result, it has become a common strategy and practice for organizations to consolidate and reduce IT assets. This typically includes reducing the number of data centers, managing all servers in a consolidated, networked environment, and modernizing and standardizing hardware and software platforms to the greatest extent possible. Budget constraints in most organizations, and particularly in government, often result in prioritization of the most cost-effective and efficient options and the elimination of redundant systems.

Consolidated organizations often implement and manage enterprise IT systems that are used throughout an entire government, across all agencies. This could include email and network domains, hardware, and software. High levels of reliability and availability are required in such situations. With limited resources and a huge amount of infrastructure, organizations must prioritize efforts to protect critical infrastructure.

[17] Lewis, 43.

Which areas are more critical than others will always be up for debate, but factors to consider include system interdependencies, redundancy, and critical nodes.[18]

Consolidation strategies usually focus on opportunities for increasing efficiency and lowering costs over several areas, as identified in Table 1. Organizations may choose any or all of these in order to completely transform the information technology environment or simply consolidate certain areas.

Table 1. Consolidation Strategies and Benefits

Area	Actions	Benefits
Infrastructure	Data center reductions	Energy efficiency; cost reduction; smaller footprint
	Increased server utilization	Cost reduction; increased efficiency
	Cloud storage	Reduction of physical assets and corresponding overhead costs
Applications	Consolidate/reduce	Cost reduction; increased efficiency; eliminate redundancy
	Standardize	More efficient to manage/maintain
	Modernize	Easier/more efficient to maintain and integrate; improved security
	Cloud	Reduction of physical assets/costs
Staffing	Pooling resources	Potential ability to cross-train and utilize as surge capacity; combined with standardized system—ability to reduce force
Governance/Procurement	Standardization	Increased efficiency and control; decreased costs

[18] Kathi Ann Brown, *Critical Path: A Brief History of Critical Infrastructure Protection in the United States* (Fairfax, VA: Spectrum Publishing Group, 2006), 9.

Federal and state government policymakers have increasingly imposed requirements to consolidate, increase efficiency, and reduce costs. In 2010, the federal Office of Management and Budget initiated an effort to reduce federal data centers, resulting in a reported closure of over 4,300 data centers by May of 2017 and reported cost avoidance or savings of approximately $2.3 billion.[19] The state of Louisiana has recently completed a consolidation of all state agency IT departments as well as certain system upgrades, claiming close to $70 million in savings.[20] The state of New York launched a consolidation initiative in 2012 and has reduced its number of data centers from fifty-three to eleven as of June of 2017, with plans to leave only two remaining.[21]

D. PROBLEM STATEMENT AND RESEARCH QUESTION

Government leaders and IT experts are not typically aware of theories and research that indicate highly connected, hyper-efficient systems contain the seeds of their own failures.[22] The consolidating and linking of so many systems may inadvertently introduce vulnerabilities that have not been considered. Information technology now underlies and connects so many basic components of daily life that its importance cannot be overstated.[23]

The Illinois state government now relies on information technology to perform everything from basic administrative tasks, such as processing employee timekeeping, to monitoring and analyzing nuclear power plant activities. Illinois' IT systems, among many other things, assist in tracking prison inmates and sex offenders, allow citizens to

---

19 *Information Technology: Sustained Management Attention to the Implementation of FITARA Is Needed to Better Manage Acquisitions and Operations*: *Testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives* (statement of David A. Powner, June 13, 2017), 12–13, https://www.gao.gov/assets/690/685231.pdf

20 Tanya Candia, "State and Local IT Leaders Target Cybersecurity in Tech Upgrades," *StateTech*, October 19, 2017, https://statetechmagazine.com/article/2017/10/state-and-local-it-leaders-target-cybersecurity-tech-upgrades.

21 Colin Wood, "'First Thing' for New New York State CIO Is Gathering the Right Team for IT Consolidation," *StateScoop*, accessed November 12, 2017, http://statescoop.com/wannacry-response-was-simple-thanks-to-consolidation-says-new-york-state-cio.

22 Ted G. Lewis, *Bak's Sandpile: Strategies for a Catastrophic World*, Kindle ed. (Williams, CA: Agile Press, 2011), loc. 32.

23 DHS, *ITSSP*.

obtain professional licenses, process taxes and fees, and run incident management and geospatial platforms to assist in real-time disaster and event response. These systems are relied upon for critical functions and activities to ensure public safety and support the citizens and economy of Illinois. A large-scale failure would be disastrous.

With this in mind, this thesis seeks to answer the following question: Consolidations of large IT systems create efficiency, but also reduce resiliency; how might a consolidated IT system remain resilient while being optimized for efficiency?

E. RESEARCH DESIGN

This thesis is focused on the potential vulnerabilities that may exist in consolidated IT systems due to the effects of complexity, self-organized criticality, and monoculture. These theories are used to analyze the consolidation in Illinois that began in 2015 in order to attempt to determine if vulnerability increases with consolidation and optimization—and, if so, the types of vulnerabilities that exist and options for mitigating them. A major component of Illinois' strategy includes heavy adoption of cloud computing, so review and analysis of potential cloud-specific vulnerabilities are also included. Using system node and link details, computer algorithms are able to produce calculations to determine a network's level of self-organization, vulnerability to cascading failures, and overall resilience.[24] This thesis provides examples of this only in order to demonstrate how self-organization, vulnerability, and resilience can be calculated. A full analysis of a system and organization as large as the state of Illinois could be done, but would require data on all nodes and links in the network and is beyond the scope of this thesis. This is not intended to produce a detailed report on specific architecture issues, but rather a higher-level analysis of current and potential weaknesses as a result of complexity and hardware and software monocultures, as well as the potential impact of heavy usage of cloud computing.

[24] Lewis, *Critical Infrastructure Protection*, 355–8.

II. THEORIES AND CONCEPTS

This chapter provides a background of the theories and issues under consideration. It begins with a brief literature review, then explains what is meant by IT consolidation, and how and why consolidations occur. The major ideas and concepts of complexity theory and self-organized criticality are then discussed without deep exploration into the math that supports components of the theories. A background on the concept of monoculture is explored, focusing on the dangers and benefits of an IT monoculture. The chapter then reviews what it means to be resilient and why resiliency has become so important when dealing with disasters.

A. LITERATURE REVIEW

The original concept that the whole is greater than the sum of its parts is often attributed to Aristotle. This idea is also part of the theory of complex systems—that the behavior or activities produced is something more than can be explained by the constituent parts. How is it that individual pieces appear to be simple and understandable, but when large events occur they are often seemingly unexplainable? Attempting to understand why some accidents become catastrophes, Charles Perrow developed normal accident theory.[25]

Smaller accidents happen regularly. However, when an accident propagates through a system of interdependent components, the severity of the event is compounded and magnified as it spreads, ultimately bringing down the entire system.[26] Normal accident theory says this unexpected behavior is inevitable due to invisible or hidden linkages. Small or relatively minor failures in a tightly coupled system can cascade in seemingly unpredictable ways with ultimately catastrophic potential.[27] So it is the linkages that are key to understanding why those small failures can have large impacts.

---

[25] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 1984).

[26] Zhang Huaxia, "Exploring Dynamics of Emergence," *Systems Research & Behavioral Science* 24, no. 4 (July 2007): 432–3, https://doi.org/10.1002/sres.845.

[27] Perrow, *Normal Accidents,* 4–5.

According to normal accident theory, accidents in complex, tightly coupled systems are not only inevitable, but the interactions that occur are often unexpected and potentially incomprehensible. This can result in inadequate response or actions taken that make the failure even worse due to the responding individuals' inability to understand what is occurring. The operators at Three Mile Island did not understand many of the system interactions that were taking place because they were not expected, which led the operator to make the wrong decisions and, ultimately, to the reactor meltdown.[28]

In 1987, Bak, Tang, and Wiesenfeld experimented with grains of sand, dropping them one by one into a pile and observing as the pile eventually collapsed into landslides. Through the experiment they demonstrated that small perturbations to a system in equilibrium have seemingly little impact until one more small change pushes it past the critical point. He referred to this as *self-organized criticality* (SOC). It is an explanation for the potential for catastrophe described by normal accident theory. Bak says that large systems with many components have the tendency to evolve into a critical state demonstrated by complex behavior, wherein seemingly minor disturbances can lead to catastrophic events.[29] As Bak states, "self-organization is an emergent process of complex systems whereby simplicity is gradually replaced by complexity."[30]

The theory of SOC has been studied to explain everything from earthquakes, traffic jams, and power outages, to the human brain. Bak's book *How Nature Works* provides examples of self-organized critical phenomena in earthquakes, volcanoes, and even life itself.[31] Research in a wide variety of areas is discovering evidence of self-organization at work.

Dr. Ted G. Lewis, in his book, *Bak's Sand Pile: Strategies for a Catastrophic World*, proposes a unifying theory as a "step toward understanding the connections

---

[28] Lewis, *Bak's Sandpile*, loc. 935.

[29] Per Bak, *How Nature Works: The Science of Self-Organized Criticality* (New York: Copernicus, 1996), 1.

[30] Lewis, *Bak's Sandpile*, loc. 185.

[31] Bak, *How Nature Work*, 89–104.

between and among complex modern systems."[32] By understanding what is causing systemic failures, we can begin to develop policies to mitigate those failures and increase resiliency.[33]

IT system consolidation is a form of SOC, which reduces resiliency. But consolidation increases efficiency, saving dollars by removing redundancy and unused capacity. Is it possible to have both? Is there a balance between efficiency and resiliency? This thesis claims it is possible to be both efficient and resilient, but IT system designers must be prepared to offset a decline in resiliency due to improved efficiency with additional vulnerability reductions to balance both.

B. INFORMATION TECHNOLOGY CONSOLIDATIONS

Government agencies have historically built independent IT structures in accordance with the needs and desires of each agency. Rather than a shared, standardized environment, agencies built their own data centers, set their own standards (or none), and built or bought multitudes of applications. And as additional equipment was purchased and new technologies emerged, old systems were not necessarily replaced. This led to IT shops with redundant systems, excess capacity, and legacy technology that can be difficult to maintain. As budgets and staff resources shrank, it thus became common strategy and practice for organizations to consolidate and reduce IT assets in an effort to be more efficient and lower operating costs. Common consolidation activities include data center and server consolidations and reductions, pooling of staff, and applications rationalization.

At least half of states have consolidated or are in some stage of consolidation or transformation.[34] The federal government has been advocating for consolidation and resource sharing among federal agencies for decades, and began to prioritize that goal in 2001 when the Office of Management and Budget identified a couple dozen of what it

[32] Lewis, *Bak's Sandpile*, loc. 23.

[33] Lewis, *Bak's Sandpile*, loc. 44.

[34] Bayard and Lee, "State Information Technology Consolidation Efforts."

called "E-Government" initiatives.[35] In 2002, Congress passed the E-Government Act.[36] The initiatives and the Act were designed to both promote and take advantage of internet-based technology. The Act recognized that interagency cooperation and interoperability are often hindered by the jurisdictional boundaries created by individual agencies, and urged transformation of agency operations by utilizing best practices from the public and private sectors.[37] Best practices in the private sector have long included outsourcing back office functions such as information technology. "Since 2004, the Treasury Department and the Office of Personnel Management have also taken steps toward leading shared services implementation across government."[38]

The Obama administration made IT shared services a priority and key initiative.[39] In 2010, the Federal Data Center Consolidation Initiative was launched to reduce the number of data centers and improve efficiency.[40] Then, in 2014, the Federal Information Technology Acquisition Reform provisions were enacted, which required agencies to report on their data center inventories and plans to consolidate and achieve savings. In November of 2015, twenty-four participating agencies had identified 10,584 data centers and, of those, had reported closing 3,125, with an additional 5,203 planned for closure by the end of federal fiscal year 2019.[41]

Concerns about IT consolidations from end users and agency leaders include loss of control and flexibility and lack of responsiveness, but there is little to no recognition of

---

35 "Presidential Initiatives," White House, accessed October 28, 2017, https://georgewbush-whitehouse.archives.gov/omb/egov/c-presidential.html.

36 E-Government Act of 2002, Pub. L. No. 107-347 (2002), accessed October 28, 2017, https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html.

37 E-Government Act of 2002.

38 Partnership for Public Service, *Helping Government Deliver II: The Obstacles and Opportunities Surrounding Shared Services* (Arlington, VA: Deloitte, 2015), 4, https://www.govexec.com/media/gbc/docs/pdfs_edit/031315cc1.pdf.

39 Steve Vanroekel, "Introducing the IT Shared Services Strategy," White House, May 2, 2012, https://obamawhitehouse.archives.gov/blog/2012/05/02/introducing-it-shared-services-strategy.

40 Government Accountability Office (GAO), *Data Center Consolidation Agencies Making Progress, but Planned Savings Goals Need to Be Established*, GAO-16-323 (Washington, DC: GAO, 2016), 1, https://www.gao.gov/assets/680/675592.pdf.

41 GAO, 3.

the potential dangers of increased complexity and/or risks of monoculture due to infrastructure and application standardization. There is some recognition of increased security risk related to data center consolidation and reduction—specifically, that consolidation puts increased pressure on remaining data centers.[42] The combination of strained budgets and the quest for hyper-efficiency often leads to concentrated assets and a system that is operated at or beyond limits, reducing surge capacity and lowering resiliency. Through consolidation, pieces of existing separate systems are joined together (coupled) and a new structure, along with SOC, emerges.[43]

The following subsections discuss examples of incidents that were facilitated due to consolidation and concentration of assets, or, conversely, would have been worse had the organization not been operating in a silo and had been tightly coupled to other systems.

1. AT&T Long-Distance Network Collapse

On January 15, 1990, a switching failure caused severe disruption to AT&T's network, and resulted in close to 50 percent of calls failing to go through.[44] The outage lasted for approximately nine hours. It was ultimately determined to have been caused by a coding error in recently updated software.[45] The tightly coupled network, however, allowed the failure in one switch to cascade throughout much of the system. Additionally, that same software was designed into a backup system that was intended to provide redundancy and higher reliability.[46] This example illustrates the inherent dangers in a

---

[42] Rick Stevenson, "Beware the Risks of Government Data Center Consolidation" *Nextgov*, August 27, 2014, http://www.nextgov.com/cio-briefing/2014/08/beware-risks-government-data-center-consolidation/92513/..

[43] Lewis, *Critical Infrastructure Protection*, 49.

[44] Dennis Burke, "All Circuits Are Busy Now: The 1990 AT&T Long Distance Network Collapse" (paper, California Polytechnic State University, 1995), http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/att_collapse.html.

[45] Burke.

[46] Karen Tumulty, "AT&T Reaches Out to Public and Apologizes for Breakdown : Telecommunications: The Firm Suspects That a 'Bug' in Computer Software Caused Its System's Collapse. It May Offer Restitution to Some and a Day of Discounted Rates to All.," *Los Angeles Times*, January 17, 1990, http://articles.latimes.com/1990-01-17/business/fi-215_1_software-systems.

tightly coupled system as well as the false comfort that redundancy can bring when it is operated in a monoculture.

2. Office of Personnel Management Data Breach

In June of 2015, federal government officials disclosed a massive data breach of the Office of Personnel Management (OPM). OPM is the human resource department for the federal government and is also responsible for managing the detailed personal information submitted by individuals seeking a security clearance.[47] The breach exposed the data of over 25 million Americans, and over 5 million individuals' fingerprints.[48]

Security clearance data resides in a database for a suite of applications known as "EPIC," and employee data resides in what is called the Electronic Official Personnel Folder (eOPF), hosted at the Department of Interior's shared services data center.[49] Both of these systems were breached. There was little segmentation in the OPM network, allowing the attackers, once they had breached the system, to move laterally throughout the environment.[50]

The attackers had access to OPM's systems for a considerable amount of time and were able to exfiltrate documents that described systems and interfaces, along with a list of contractors who had access to certain systems.[51] U.S. Investigations Services, an OPM background investigation contractor, acknowledged a data breach of its systems in August 2014, resulting in personally identifiable information (PII) for 31,000 individuals

---

[47] David Kennel, *OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster* (North Bethesda, MD: The Sans Institute, 2016), 2, https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852.

[48] Kennel.

[49] Sean Gallagher, "'EPIC' Fail—How OPM Hackers Tapped the Mother Lode of Espionage Data," *Ars Technica*, June 22, 2015, https://arstechnica.com/information-technology/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.

[50] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation: Majority Staff Report Committee on Oversight and Government Reform, U.S. House of Representatives*, 114 Cong (September 7, 2016), 76, https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[51] H.R., 66.

being compromised.[52] Another contractor, KeyPoint, was found in December 2014 to have been breached as well, with possible PII compromised for over 48,000 individuals. The credentials of a KeyPoint employee with an OPM account were compromised during this breach and, according to testimony by KeyPoint CEO Eric Hess, were used to gain access to OPM.[53]

There are multiple documented failures by OPM in basic cyber-hygiene practices that contributed to the breaches. They include lack of multi-factor authentication, which requires physical possession of a chip-enhanced ID card and would have made unauthorized access using stolen usernames much more unlikely.[54] Almost half of OPM's forty-seven systems were owned by contractors; OPM had limited oversight of the systems and conducted limited monitoring.[55] Office of the Inspector General reports found unpatched servers, which can leave holes for attackers to enter through. Data was not encrypted, something that OPM's director blamed on legacy systems that could not feasibly be encrypted.[56] Although legacy systems can be encrypted, it may be more difficult and expensive to do so. OPM also had gaps in its logging capabilities, which made it impossible to definitively determine the attackers' entry point or know for certain everything that may have been compromised.[57]

Again, all of these deficiencies were contributors to the magnitude of the breach, but the number of systems linked together, along with the lack of segmentation, allowed the attackers to enter OPM's environment, drop malware that allowed them to persist throughout the network, and then move laterally into the shared services data center at

---

[52] H.R., 31.

[53] H.R., 32.

[54] H.R., 77.

[55] Institute for Critical Infrastructure Technology, "Handing Over the Keys to the Castle. OPM Demonstrated That Antiquated Security Practices Harm National Security" (report, Institute for Critical Infrastructure Technology, 2015), 10, http://icitech.org/wp-content/uploads/2015/07/ICIT-Brief-OPM-Breach2.pdf.

[56] H.R., *The OPM Data Breach*, 47.

[57] H.R., 72.

Department of the Interior, which housed OPM personnel records.[58] While poor cyber hygiene was a component of the OPM breach, the consolidation and centralization of the federal IT systems magnified the consequences. Once the hackers found a way in, they were able to take advantage of that centralization to access millions of consolidated records.

3. Illinois State Board of Elections Attack

In July of 2016, the Illinois State Board of Elections became aware of an attack on the Illinois Voter Registration System database.[59] Through an SQL injection attack, the information of up to an estimated 90,000 Illinois voters was hacked, most likely by foreign actors.[60] While concerns were immediately raised about foreign adversaries altering U.S. elections, the Illinois voter registration database is maintained separately from each county's voter rolls. It has recently been reported that systems in thirty-nine states were targeted and hit by hackers.[61] Luckily for the country as a whole, "the American voting system, with its hodgepodge of state and local polling places, is protected by being decentralized and disconnected."[62] So, while we often seek to connect systems together in search of efficiency and effectiveness, that is fortunately not the case for the U.S. election system, where a nationwide, networked system may have been much more vulnerable to manipulation. This example illustrates the virtue of a distributed, disconnected, "inefficient system," if attacked by malware.

---

[58] H.R., 83.

[59] Illinois State Board of Elections, "Illinois Voter Registration System Database Breach Report" (report, Illinois State Board of Elections, 2016), 1, www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_26_16AgendaAmended.pdf.

[60] "After 2016 Election Hacking, Illinois Politicians Pose Cybersecurity Questions to Local Officials," *Cyberscoop* (blog), June 16, 2017, https://www.cyberscoop.com/after-2016-election-hacking-illinois-will-assess-election-system-cybersecurity/.

[61] "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 13, 2017, https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[62] David E. Sanger and Charlie Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System," *New York Times*, September 14, 2016, https://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html.

C. COMPLEXITY

Describing something as "complex" means that the whole is greater than the sum of its parts. A system is complex when its parts interconnect in intricate ways that may not be fully understood. However, complexity is not the same as chaos. Chaos is defined by complicated and random behavior from the iteration of a simple rule.[63] "Complexity is the generation of rich, collective dynamical behavior from simple interactions between large numbers of subunits."[64]

Simple systems are composed of few parts and are easily knowable and predictable. Complicated systems have many parts and are still knowable, although they are not as simple. Complex systems are not fully knowable and evolve more than they are engineered.[65] Complexity theory describes analytical methodologies used in various disciplines, including physics, mathematics, and biology. The theory assumes that complex systems are not in a state of equilibrium, but are perched near breakdown.[66] Once perched at this self-organized critical state, a small change anywhere in the system could lead to a chain reaction of events that impact the whole system.

When systems become complex, they often behave in unexpected ways as they adapt to their environment. This complexity emerges from self-organizing behavior.[67] Those behaviors only occur when the system is observed in its whole and would not be identifiable in any of its individual parts.[68] As noted by Paczuski and Bak, "this

---

[63] Dean Rickles, Penelope Hawe, and Alan Shiell, "A Simple Guide to Chaos and Complexity," *Journal of Epidemiology and Community Health* 61, no. 11 (November 2007): 934, https://doi.org/10.1136/jech.2006.054254.

[64] Rickles, Hawe, and Shiell, 934.

[65] "Simple vs. Complicated vs. Complex vs. Chaotic," *NOOP.NL* (blog), August 20, 2008, http://noop.nl/2008/08/simple-vs-complicated-vs-complex-vs-chaotic.html.

[66] Cristoforo Sergio Bertuglia and Franco Vaio, *Nonlinearity, Chaos & Complexity: The Dynamics of Natural and Social Systems* (New York: Oxford University Press, 2005), 282.

[67] Maya Paczuski and Per Bak, "Self-Organization of Complex Systems," Cornell University Library, June 5, 1999, 1, http://arxiv.org/abs/cond-mat/9906077.

[68] Bertuglia and Vaio, *Nonlinearity, Chaos & Complexity*, 272–3.

irreducibility is what makes systems complex."[69] To understand emergence, consider the features found in Table 2.

Table 2. Features of Emergence[70]

Wholeness	The whole produces properties or functions that do not occur or exist in the components independent of the whole.
Novelty	New properties continuously arise through an evolutionary process
Downward Causality	When the wholeness of the system arises, it forces components to change behaviors and functions in order to follow the laws of higher levels.
Unpredictability	The behaviors or patterns of emergence cannot be predicted based upon behaviors of pre-existing components.
Irreducibility	Emergence is unpredictable from its components but also not completely deductible to its components after the behavior or properties arise.

The process appears to be emergent or self-organized due to the gradualness of the changes occurring, but it requires some type of force or energy acting on the system. Movements in the Earth's crust leading to earthquakes or policy decisions that shape an IT environment are examples. As we find imperfections in a system, we continually make adjustments and improvements in order to optimize it.

Dr. Ted G. Lewis asserts that "self-organized systems are typically nonredundant, nonsurge capable, single-point-of-failure systems with bottlenecks, overly concentrated assets, and inadequate backup capacity."[71] Natural and manmade catastrophes are byproducts of normal complex system behaviors.[72] Small incidents cascade and become magnified as they travel through system linkages.

---

[69] Paczuski and Bak, "Self-Organization of Complex Systems," 4.

[70] Adapted from Huaxia, "Exploring Dynamics of Emergence," 432–3.

[71] Lewis, *Critical Infrastructure Protection*, 43.

[72] Ted G. Lewis, Thomas J. Mackin, and Rudy Darken, "Critical Infrastructure as Complex Emergent Systems," *International Journal of Cyber Warfare and Terrorism (IJCWT)* 1 (January–March 2011): 3, http://dx.doi.org/10.4018%2Fijcwt.2011010101.

Complex systems are often modeled as a network containing nodes, links, and a wiring topology that describes how links are used to connect pairs of nodes. Nodes represent system components and the links represent interactions between the components. System hubs are nodes with a higher-than-average number of links and are more critical than nodes with fewer links. It is the links in a system that can allow failures to spread throughout. With increasing connectivity (either through link density or hub size), SOC increases as well.[73] Link density is also referred to as percolation. The more tightly coupled, or linked, various elements of a system are, the more damaging any disruption could be to the system. Networks evolving through continual addition of links and rewiring to optimize the network can become increasingly self-organized.[74] The denser the network connections become, the closer it will come to maximum capacity, and the closer it will come to the critical point.[75]

Networks are typically classified by how the links are distributed among pairs of nodes. Random networks are just that—formed by randomly connecting pairs of nodes.[76] Scale-free networks contain a hub with a great number of connections as well as many nodes that have few connections.[77] Figure 1 provides simple, representative models of a random network and scale-free network. They are useful for studying the behavior of coupled (linked) systems, which is the method through which failures cascade.

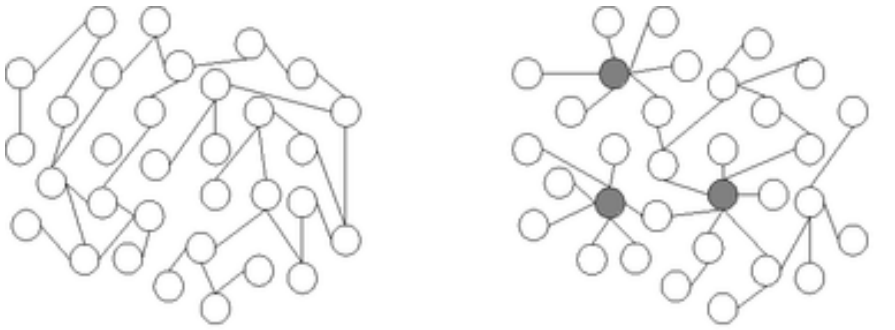
[73] Lewis, *Bak's Sandpile*, loc. 1192.

[74] Lewis, loc. 1093.

[75] Lewis, loc. 1093.

[76] Lewis, *Critical Infrastructure Protection*, 64.

[77] Lewis, 65.



(a) Random network (b) Scale-free network

Figure 1. Network Types[78]

Scale-free networks, those that contain many nodes with only a few connections along with one or two hubs that have a disproportionate number of connections, are more self-organized and therefore the least resilient. Hub-like structure can occur through preferential attachment, which creates concentration of assets and critical hubs, which are vulnerable.[79] These types of networks "are prone to rapid propagation of faults, because hubs are super-spreaders: nodes that accelerate and magnify the spread of faults."[80]

Preferential attachment is a property of self-organizing networks. Random networks self-organize into scale-free networks as they evolve over time. This is due to many factors, but in the context of this thesis the drivers of self-organization are reduction of redundancy and cost-saving efficiency. Lewis quantifies the two main drivers of self-organizing networks—percolation and preferential attachment—into a single quantity called spectral radius, r. As SOC increases, so does r. Thus, r is a useful measure of self-organization.

78 Source: Wikipedia, s.v. "Scale-Free Network," December 13, 2017, https://en.wikipedia.org/w/index.php?title=Scale-free_network&oldid=815200489.

79 Lewis, *Critical Infrastructure Protection*, 44.

80 Lewis, *Bak's Sandpile*, loc. 1645.

D. MONOCULTURE

Monoculture is a term that is used to describe a system that has little to no diversity. For instance, in agriculture, monoculture is the practice of growing only a single crop. Monocultures in nature, such as a species with little to no genetic diversity, are rare because they are vulnerable to a single attack and thus risk extinction.[81] In a biological system, genetic diversity is what ensures much of the population will survive. But in a monoculture, if the dominant species or crop variety is susceptible to a specific threat, it has the potential to wipe out the entire population. The Irish potato famine is an example of a single crop species with little to no genetic diversity, all vulnerable to the same disease which ultimately destroyed the crops throughout Ireland.[82] Consolidated IT environments tend to standardize hardware and software, creating a monoculture. While this is desirable in terms of cost savings, efficiency, and interoperability, the monoculture system will share vulnerabilities, which puts the whole system at risk.[83] Monoculture in nature risks extinction of a population; diversity helps to ensure survival of a population.

The elimination of competition and diversity also may lead to a loss of resilience. The interconnectedness and standardization of systems, which allows the easy exchange of information within an organization, also produces a situation that allows the efficient spread of malware throughout the entire system.[84] Software monoculture (systems running mostly the same software) can be a threat to resilience.[85] In a monoculture, an attack on one part is an attack on all parts, enabling large-scale failure.

It has also been argued, however, that monoculture with strategically chosen diversity built in can reduce risk, but an organization must take into consideration the

---

[81] Kenneth P. Birman and Fred B. Schneider, "The Monoculture Risk Put into Context," *IEEE Security & Privacy* 7, no. 1 (February 2009): 14–17, https://doi.org/10.1109/MSP.2009.24.

[82] "Monoculture and the Irish Potato Famine: Cases of Missing Genetic Variation," Berkeley, accessed February 2, 2018, https://evolution.berkeley.edu/evolibrary/article/agriculture_02.

[83] Jaynarayan Lala, "IT Monoculture Security Risks and Defenses," *IEEE Security & Privacy* 7, no.1 (2009): 12.

[84] Birman and Schneider, "Monoculture Risk."

[85] Daniel Williams et al., "Security through Diversity: Leveraging Virtual Machine Technology," *IEEE Security & Privacy* 7, no. 1 (2009): 26.

costs and benefits of doing so. Monoculture risks can be mitigated and may be easier to defend than the complexity created by introducing diversity.[86] Diversity is expensive and consumes more staff resources; however, some form of diversity may be worth the cost, particularly for mission-critical systems.

E. RESILIENCE AND EFFICIENCY

Resilience, as defined by DHS, means the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[87] A system's resilience "depends on the ability to mitigate an unusually disruptive event that may produce a harmful outcome."[88] For IT environments, unwanted, harmful outcomes include anything that results in reduction or loss of service, data, or security. As a system grows in size and complexity, the individuals who maintain it are more likely to be specialists in particular areas, rather than generalists who understand the system as a whole. This compounds the problem of understanding what is happening in a system when something goes wrong. The increased complexity adds increased difficulties for those trying to establish resilience.[89]

When the IT environment is small and only loosely connected, the impacts of a disruptive event are relatively limited. But for organizations operating tightly coupled, consolidated infrastructure, the consequences may be magnified due to SOC and the cascading impacts of linked systems and software monoculture. With limited resources available, DHS focuses on and advocates for implementing measures that enhance security and increase resilience.[90]

Efficiency can be defined as producing something without waste. Most organizations today strive to be as efficient as possible and typically centralize functions

---

[86] Birman and Schneider, "Monoculture Risk," 15.

[87] DHS Risk Steering Committee, *Risk Lexicon*.

[88] Chris C. Demchak, "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)," *Journal of Comparative Policy Analysis: Research and Practice* 14, no. 3 (2012): 255, https://doi.org/10.1080/13876988.2012.687619.

[89] Demchak, 255.

[90] DHS, *ITSSP*, 13.

in order to do so. Redundant capabilities and excess capacity are often reduced or eliminated in order to save money. And this efficiency leads to fragility. But resilience requires excess capacity, often referred to as surge capacity. Many organizations today keep on hand only what is anticipated to be needed, on average, to keep operations running. They rely on just-in-time deliveries in order to avoid carrying the cost of stockpiling assets. But what happens if the there is a breakdown somewhere in the supply chain? It propagates through the chain, ultimately impacting the organization. In order to be resilient, the organization should maintain some amount of excess.

It is the same for IT systems. Extreme optimization that runs systems at maximum capacity is more efficient, but cannot handle a surge in demand, which can ultimately cause widespread overload and failure. The conundrum is that efficiency sacrifices resilience, and to gain resilience you must sacrifice efficiency. Thus, efficiency and resilience must be balanced.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ILLINOIS IT TRANSFORMATION

Illinois embarked on IT transformation in 2015. While IT consolidation is a process of optimizing systems in order to improve performance while simultaneously reducing costs, IT transformation typically goes further than consolidation, involving not just consolidation of assets, but a reimagining of the way the organization operates. IT transformation typically includes redesigning the organization, rethinking how technology supports the business, and developing a strategy to implement those changes. With that transformation inevitably comes consolidation of infrastructure, staff, networks, applications rationalization, and a drive toward enterprise solutions.

Illinois first attempted consolidation of state information technology functions beginning in 2004. The consolidation was only partially completed and focused on hardware and network services. In 2016, the state of Illinois created a new state agency responsible for all IT functions, the Department of Innovation and Technology (DoIT), for executive branch agencies and launched a new effort to not just consolidate IT infrastructure, but to modernize the technology, standardize applications, and implement an enterprise architecture.[91] While Illinois' IT transformation is broad in scope—encompassing establishment of a new agency, staff consolidations, financial and procurement process improvements, and service improvement—this section focuses specifically on infrastructure technology, software, and standardization. Illinois' IT environment has evolved over time and is broken primarily into two phases, the current state, which is an assessment of the environment as it existed in 2015, and the future state, the desired future IT environment.

A. CURRENT STATE

In 2015, Illinois' information technology environment was partially centralized as a result of an earlier attempt at consolidation in 2004. At that time, twenty-two of fifty-seven state agencies had their infrastructure consolidated and managed by the Illinois Department of Central Management Services (CMS), while an additional twenty-five

[91] Illinois Office of the Secretary of State, *Executive Order 2016-01*.

were not consolidated but received some services from CMS.[92] The agencies consolidated as part of the earlier effort had the majority of their infrastructure housed in the centralized data center within CMS. All agencies' applications development staff and support operations remained within each agency's individual IT department.

Illinois agencies maintained several data centers in multiple geographically dispersed locations, several mainframes, and thousands of midrange servers. Three of the data centers contained approximately 80 percent of all servers, with the remaining 20 percent spread out across over 200 addresses in 102 cities.[93] There were found to be about an equal number of physical and virtual servers with nearly half running different versions of Microsoft operating systems, with a mix of other operating systems on the remainder.[94] Hardware was also from a variety of manufacturers, HP the most predominant but also Lenovo and Cisco. On top of this infrastructure, state agencies were running about 2,800 separate applications in numerous languages, including a large number in Visual Basic related, C related, and COBOL.[95] Most applications were custom built in house.

The backbone of Illinois' network is the Illinois Century Network, a public, high-speed broadband network managed by the Illinois DoIT. The Illinois Century Network maintains fifteen points of presence and supports internet connectivity for thousands of schools, libraries, universities, and state and local governments throughout Illinois.[96]

The 2004 consolidation was primarily an attempt to reduce spending and resulted in not just a lack of investment, but a deliberate reduction in spending, which ultimately impacted service quality. Agencies avoided further consolidation and continued to build their own infrastructure and applications, designed around their own standards.

---

[92] Deloitte, "State of Illinois Current State Assessment" (report, State of Illinois, 2016), 66–68, https://www2.illinois.gov/sites/doit/Strategy/Transformation/ProgramWiki/Documents/CurrentStateAssessment.pdf.

[93] Deloitte, 71.

[94] Deloitte, 72.

[95] Deloitte, 89.

[96] "Illinois Century Network," State of Illinois, accessed November 26, 2017, www.illinois.gov/icn/Pages/default.aspx.

Overall, a variety of architecture and lack of statewide governance, along with siloed technology operations, had created large inefficiencies, inadequate staffing, and a fragmented IT environment. With so many legacy systems running, it is often the case that only one or two staff members have the necessary skills to support them. The age of the systems makes them fragile and the lack of adequate staff with the skills necessary for support creates unacceptable risk. These systems are also difficult to extend or integrate with others and often do not support the modern environment users and citizens desire, such as online and mobile access. Maintaining so many different databases, applications, and infrastructures is a huge time sink for staff and often prevents deployment of newer, more useful technologies.

B. FUTURE STATE PLAN

To improve efficiency, security, and user experience while lowering the overall cost of doing business, the state defined a future or end-state vision of its IT environment and documented a strategy to get there. This plan includes an enterprise governance model to reduce siloes and support interoperability, reduce the number of data centers and servers, and employ fewer applications while also standardizing software platforms. These actions are intended to create a more efficient environment that is easier and less costly to support.

All agency servers, security, network, storage, and database infrastructure are to be consolidated into the DoIT data center.[97] Enterprise application standards will be implemented in order to standardize software languages and reduce the number of applications. Applications will be reduced and legacy technologies will be re-platformed in enterprise-wide applications whenever possible.[98] And finally, Illinois' desired future state includes deploying a "cloud first" strategy for backup, storage, testing, and

[97] Deloitte, "State of Illinois—IT Transformation Future State Recommendations" (report, State of Illinois, 2016), 28.

[98] Deloitte, 24.

applications development, with a goal to have 70 percent of the workload in the cloud by 2018.[99]

There are four general operating models to describe the "level of process integration and standardization in a given organization."[100] The models are described in Figure 2. Illinois was operating within the "diversification" model. The desired future state is somewhere between coordination and unification. Core processes should utilize enterprise-wide systems, common processes among agencies should utilize standardized or shared solutions, and custom applications should be extremely limited.

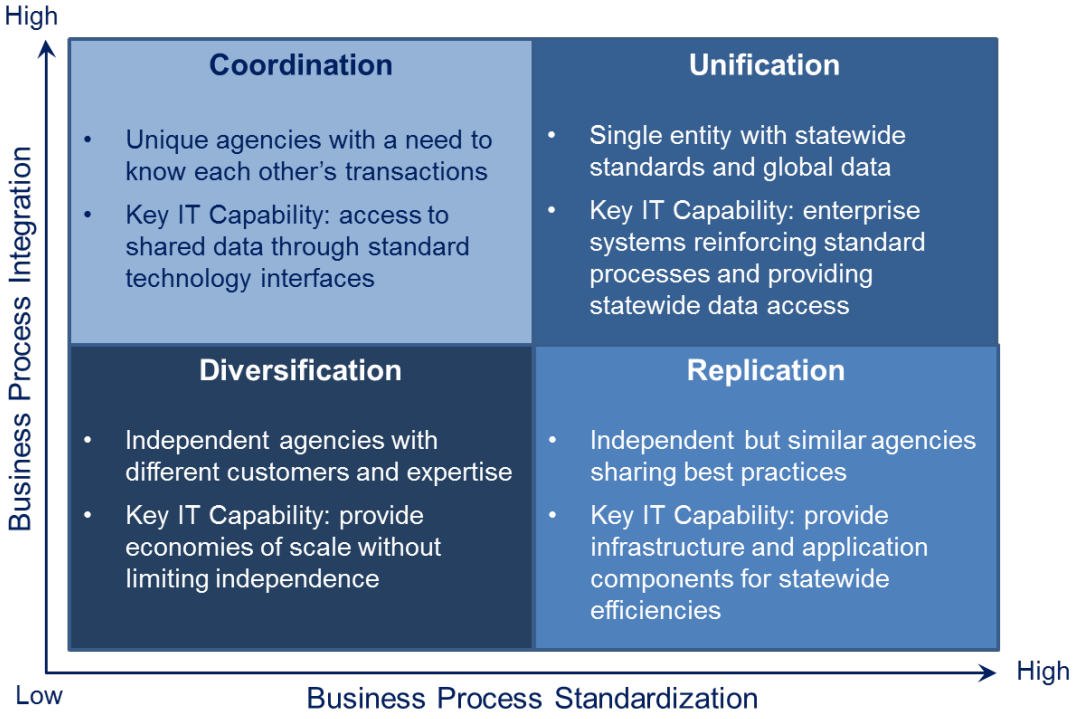


Figure 2. Enterprise Operating Model[101]

[99] Deloitte, 31.

[100] Deloitte, "IT Transformation Future State Enterprise Architecture Strategy," (report, State of Illinois, 2016), 38.

[101] Source: Deloitte, 38.

A large part of Illinois' strategy for a more centralized and efficient operation includes heavy use of the cloud. Cloud computing is the latest strategy in the quest for increased efficiency and reduced costs in IT organizations. Utilizing the cloud for storage and delivery of applications allows organizations to avoid large investments in infrastructure and unused, excess capacity. Organizations can then reduce or expand their usage based upon current needs, operating in the most efficient manner possible. The increased amounts and availability of bandwidth have made cloud services viable only relatively recently. Defining the cloud has often been the subject of discussion over the years, but NIST defines it as follows:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[102]

Service models generally fall into the following categories[103]:

- Software as a Service (SaaS)—software applications are hosted on the provider's infrastructure and accessed by the user through a thin client interface.
- Platform as a Service (PaaS)—allows the client to access the cloud infrastructure in order to develop, manage, and deploy applications.
- Infrastructure as a Service (IaaS)—the provider hosts the infrastructure and the user has the ability to provision processing, storage, networks, and other resources.

Deployment models include public, private, or a hybrid of the two. A public cloud is available to the general public over the internet and is owned and operated by a provider with the infrastructure maintained somewhere other than the consumer

---

[102] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Gaithersburg, MD: NIST, 2011), 2, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-145.pdf.

[103] Mell and Grance, 2–3.

location.[104] A private cloud is one exclusively for a single organization and may be hosted on or off premises and managed by either a third party or the organization.[105]

Prior to the first consolidations, the state's IT environment was highly decentralized and somewhat siloed. Today it is becoming increasingly centralized but has not yet moved to the full centralization of the desired end state, encompassing all infrastructure, applications, and staff. The current Illinois IT environment is evolving toward a highly centralized and optimized environment and will likely move toward a scale-free system, losing resiliency along the way. Scale-free networks are typically less vulnerable to random failures but much more vulnerable to targeted attacks.[106] Scale-free networks, because of their structure, are also vulnerable to cascading failures.[107] Because all components are linked through a centralized hub, it is much easier for malware to spread.

In terms of the research question posed in Chapter I, centralization is a form of SOC, which reduces resilience to targeted attacks. As the Illinois IT system evolves from a diverse, decentralized, redundant collection of IT assets toward a monoculture, centralized, cloud-based, efficient collection of IT assets, it also becomes less resilient unless other measures are taken to reduce vulnerabilities. Centralization in a single data center or in the cloud and standardization of hardware and software systems increase the risks associated with a monoculture unless mitigated by greater security and tighter control of access by authorized users.

---

104 Wayne Jansen and Timothy Grance, *Guidelines on Security and Privacy in Public Cloud Computing*, Special Publication 800-144 (Gaithersburg, MD: NIST, 2011), 3, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

105 Jansen and Grance.

106 A. L. Barabasi, "The Architecture of Complexity," *IEEE Control Systems* 27, no. 4 (August 2007): 37, https://doi.org/10.1109/MCS.2007.384127.

107 Barabasi, 38.

IV. ANALYSIS

This chapter delves into some of the mathematics involved in network theory and how it is used to model and study systems. This provides a means to quantify self-organization, determine systems vulnerability and resilience, and to help understand how to mitigate the vulnerabilities identified. It is the system's structure that determines how resilient the system is, not simply each component's weakness (remember, the whole is greater than the sum of its parts). We also apply these means to a representative example from Illinois specifically, but it could be used as an example for any system being centralized.

A. QUANTIFYING SELF-ORGANIZATION

Complex systems typically display properties captured by probability distributions when observing large numbers of events. Plotting the observed events produces an exceedence probability curve that is typically a power law. Exceedence probability measures the likelihood that an event will exceed a particular consequence.[108] Power laws represent functional relationships between two quantities. A change in one results in a proportional change in the other. Essentially, this means that small events are much more likely than extreme events.[109] An exponent determines the rate of decline, represented as q.[110] The larger the exponent, the more frequent the events are at the low end of the consequence scale and the less frequent they are at the high-consequence end of the scale.[111] This is what Bak, Tang, and Wiesenfeld observed during the sandpile experiment. They observed small landslides much more frequently than large ones, following a power law curve. The objective of system design is to create a system with a corresponding exceedence probability curve with q as large as possible, because fewer extreme incidents happen for larger values of q.

---

108 "Cause-and-Effect or Fooled by Randomness?," *Homeland Security Affairs* (blog), January 1, 2010, https://www.hsaj.org/articles/93.

109 Lewis, *Critical Infrastructure Protection*, 345.

110 Lewis, *Bak's Sandpile*, loc. 136.

111 Lewis.

There are two contributing factors to SOC: link density and node connectivity. As link density and/or node connectivity increase, so does SOC. A mathematical quantity called the spectral radius, r, is used to quantify SOC.[112] SOC and r increase with link density and hub size. Higher spectral radius means SOC is present and the higher the spectral radius, the higher the risk.[113] Most importantly, higher values of r mean lower values of resilience.

Vulnerability, v, is defined as the probability of collapse when an asset such as a hardware or software component is stressed. System vulnerability relates to stresses such as monoculture, surge capacity, and weakness in nodes or links. Higher values of vulnerability (v) mean lower values of resilience, also. When we combine spectral radius and vulnerability into a product, vr, we combine the effects of SOC with the effects of stresses into a single measure of fragility.

Dr. Ted G. Lewis showed that cascade resilience decreases with an increase in both vulnerability (v) and spectral radius (r).[114] Here, v is a measure of the probability of a node failing due to the failure of a neighboring node.[115] Consider an IT system under attack by malware, which spreads like a virus from one asset to another. Such spreading is a form of cascading, and according to the simple measure of fragility presented here, cascade resilience increases with a decrease in vr. Therefore, system resilience is counter-proportional to vr:

$$S \sim -vr.$$[116]

Typical actions that occur while consolidating IT systems are represented in Tables 3 and 4, with their effects on vulnerability and spectral radius.

---

[112] Lewis, loc. 1460.

[113] Lewis, loc. 1460.

[114] Lewis, *Critical Infrastructure Protection*, 357.

[115] Lewis, 65.

[116] Lewis, 65.

Table 3. Vulnerability

Cause	Effect
Increased monoculture	Increases
Reduced surge capacity	Increases
Software flaws	Increases

Table 4. Spectral Radius

Cause	Effect
Increased hub size	Increases
Increased connection density	Increases

Resiliency has an inverse relationship with vr—it decreases as vr increases.[117] So, while high-consequence, extreme events happen less frequently than smaller-consequence events, with increased vr the big events will be even more damaging.[118] The objective of resilient system design is to reduce v, r, or both.

B. STATE OF ILLINOIS

Prior to the first attempt at IT consolidation in Illinois, the Department of Central Management Services (CMS) housed and managed several core mainframe servers, which supported legacy applications. These applications include financial and accounting programs, payroll, personnel, timekeeping, and asset tracking. Many of these were used only by CMS, but some of the applications were used by multiple agencies. The majority of agencies housed and maintained their own hardware, network domains, and applications with little to no connectivity between and among agencies.

[117] Lewis, *Bak's Sandpile*, loc. 861.

[118] Lewis, loc. 872.

After 2004, the state initiated the first consolidation efforts, which were primarily focused on consolidating physical servers in a "lift and shift," meaning servers were physically removed from approximately a dozen agencies and shifted to the CMS data center and connected to the CMS network domain. By 2008, the CMS data center housed approximately 1,400 servers. The majority of these were physical, separate servers and around 200 were virtualized blade servers. These agencies were now linked together, their servers and applications housed within the state data center. The core servers in the data center remained and were now linked to agency server farms co-located. Each agency now has hundreds or thousands of connections between agency hardware in use to the servers in the CMS data center. Both link density and hub size were beginning to increase.

As the data center continued to be modernized, optimized, and re-wired, by 2010 the physical servers were consolidated further. Where there were once close to one thousand physical servers, this was reduced to approximately 200 physical servers and about 1,000 virtualized blade servers. In addition to the twenty-two agencies that already have consolidated infrastructure in the CMS data center, an additional thirty-five that were not consolidated had varying levels of connection or support from CMS through such instances as links to the Illinois Century Network for internet connectivity or shared applications.

A recent example of a portion of the Illinois network was analyzed for resilience by simulating cascades initiated by failure of a randomly chosen node. For example, a failure might be the spreading of malware. Figure 3 represents the Illinois network approximately as it stands now. Figure 4 is a representation of what the Illinois network may look like after consolidation and centralization. In both figures, self-organization is quantified by spectral radius, r.[119]

The spectral radius of the network in Figure 3 is 3.03, which is considered low. A purely random network of this size would have a spectral radius of 2.8, indicating no self-

[119] Lewis, *Critical Infrastructure Protection*, 357.

organization.[120] As consolidation increases the connectivity of a central node—such as a central server in the data center—spectral radius increases. For example, in Figure 4, spectral radius is 4 because the hub is connected to seventeen links. Therefore, Figure 4 is more organized than Figure 3. Consolidation raises spectral radius from 3.03 to 4.0.

The future state plan to centralize all IT operations and assets in one data center or cloud offering, with one backup location, would look like Figure 4.

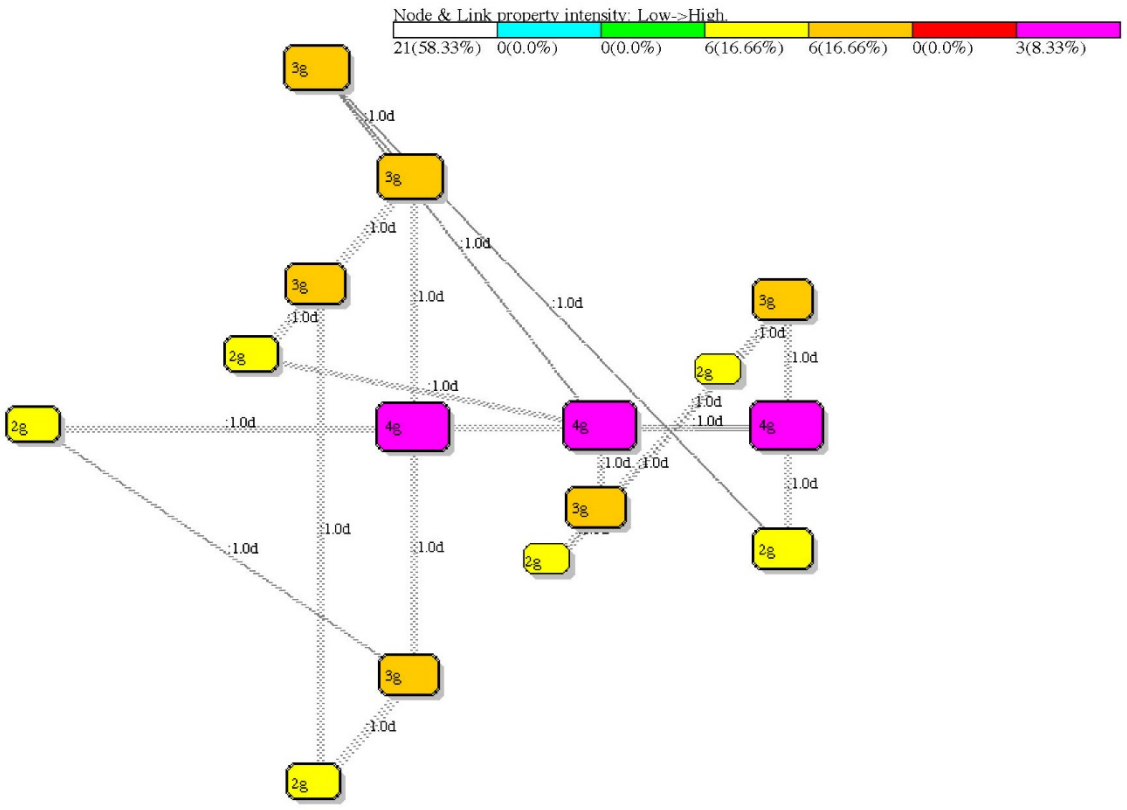


Figure 3. State of Illinois Network circa 2015[121]

[120] Lewis, 65.

[121] Image courtesy of Dr. Ted G. Lewis.

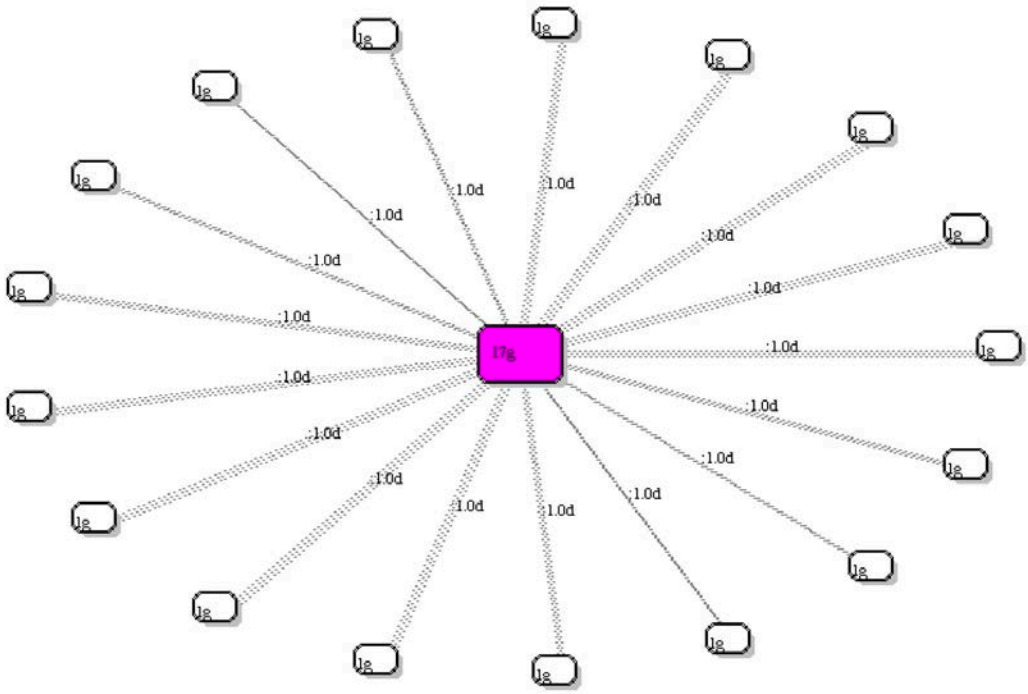


Figure 4. Illinois Future State Representation[122]

[122] Image courtesy of Dr. Ted G. Lewis.

Figure 5 shows how resilience of the network in Figure 4 declines as vulnerability (v) increases from zero to one. Risk increases as this calculation approaches one, becoming prone to catastrophic failures when that number is significantly greater than one.[123]

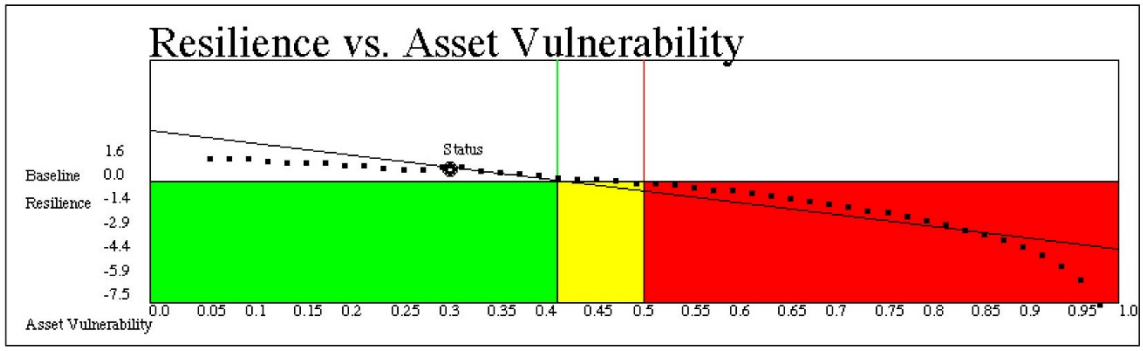


Figure 5. Network Resiliency[124]

If v is known, we can locate the Illinois network on this sloping line to determine its resilience. However, that is unnecessary for this analysis because we are simply showing that resilience declines as consolidation moves toward the hub-and-spoke network shown in Figure 4.

C. CONSOLIDATION IN THE CLOUD

Cloud computing is subject to the same general threats and vulnerabilities as an organization's locally owned and administered computing environment. However, additional challenges exist when hardware, software, and data storage are outsourced to a third party. Much of what makes cloud computing attractive is also cause for concern in regards to security and control. But how much of the concern is simply a fear of the unknown? While the magnitude of potential loss does not change simply due to cloud computing, it is possible that there could be a change in vulnerability and threats. Are there vulnerabilities specific to using the cloud that may not otherwise be found in a

[123] Lewis, *Critical Infrastructure Protection*, 65.

[124] Image courtesy of Dr. Ted G. Lewis.

traditional IT infrastructure? Proposed indicators of cloud-specific vulnerabilities follow. To be cloud-specific, they must be:

- intrinsic to or prevalent in cloud computing technology,
- rooted in one of NIST's cloud characteristics,
- caused when cloud innovations make it difficult or impossible to implement, or,
- prevalent in even the best cloud offerings.[125]

Vulnerabilities specific to these indicators are identified in Table 5.

Table 5. Cloud-Specific Vulnerabilities[126]

Indicator	Vulnerability
Intrinsic cloud technology vulnerabilities	Virtual machine escape
	Session riding and hijacking
	Insecure/obsolete cryptography
Rooted in NIST's cloud characteristics	Unauthorized access to management interface
	Internet protocol vulnerabilities
	Data recovery vulnerability
	Metering and billing manipulation
Cloud innovation causes difficulty in implementing security controls (control challenges)	Insufficient network-based controls (IP-based network zoning cannot be applied; network-based vulnerability scanning usually forbidden)
	Poor key management procedures
	No standardized cloud-specific security metrics customers can use to monitor security status of their cloud resources
Prevalent in the best cloud offerings	Injection vulnerabilities exploited by manipulating service or application inputs
	Weak authentication mechanisms

[125] Bernd Grobauer, Elmar Stocker, and Tobias Walloschek, "Understanding Cloud Computing Vulnerabilities," *IEEE Security & Privacy* 9, no. 2 (April 2011): 52.

[126] Grobauer, Stocker, and Walloschek, 52–54.

Many of the most well-known cloud computing failures have been caused by a variety of failures that could impact any IT operation, but when the organization lacks control over the service being provided and has no failover backup, it is at the mercy of the cloud provider to get the service back up and running. In 2014, Dropbox suffered a significant outage as a result of a failed upgrade.[127] Salesforce was down for nine hours in July of 2012 due to a brief power outage at the data center run by a cloud provider.[128] GitLab not only suffered an eighteen-hour service outage in January of 2017 due to an employee mistake during server maintenance, but customer production data was lost and unable to be recovered as well.[129] In February of 2017, what was intended to be minor maintenance on a small number of servers at Amazon Web Services ended up impacting far more servers than anticipated and took down many customers for several hours.[130]

Cloud security is a common concern, but many well-known breaches have been the result of simple configuration errors. In 2017, the U.S. Department of Defense accidentally exposed files stored in Amazon's cloud storage service because of a mistaken configuration that allowed any Amazon Web Services user to view the files.[131] Some of these files were labeled as "Top Secret" and "NOFORN," indicating they contained extremely sensitive intelligence information.[132] And a misconfigured database is also said to be the cause of the exposure of personal information of close to 200 million American voters discovered in June of 2017.[133] Again, this information was stored in an

---

127 "Top 20 High Profile Cloud Failures of All Time," Techflier, accessed February 9, 2018, https://www.techflier.com/2016/01/25/top-20-high-profile-cloud-failures-all-time/.

128 Techflier.

129 Joseph Tsidulko, "The 10 Biggest Cloud Outages of 2017 (So Far)," CRN, August 1, 2017, http://www.crn.com/slide-shows/cloud/300089786/the-10-biggest-cloud-outages-of-2017-so-far.htm.

130 Jason Del Rey, "Amazon's Massive AWS Outage Was Caused by Human Error," *Recode*, March 2, 2017, https://www.recode.net/2017/3/2/14792636/amazon-aws-internet-outage-cause-human-error-incorrect-command.

131 "Pentagon Left AWS Databases Publicly Exposed," *Cyberscoop* (blog), November 17, 2017, https://www.cyberscoop.com/dod-amazon-web-services-exposed-data-chris-vickery/.

132 Dan O'Sullivan, "Black Box, Red Disk: How Top Secret NSA and Army Data Leaked Online," *UpGuard* (blog), updated November 28, 2017, https://www.upguard.com/breaches/cloud-leak-inscom.

133 Dan O'Sullivan, "The RNC Files: Inside the Largest U.S. Voter Data Leak," *UpGuard* (blog), updated December 20, 2017, https://www.upguard.com/breaches/the-rnc-files.

Amazon Web Services storage bucket that was misconfigured to allow anyone to access the data.[134]

Cloud computing suffers from the same threats and vulnerabilities as most IT environments. Being entirely web-based is cause for additional awareness of the business impact should connectivity be lost.

[134] O'Sullivan.

V. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSION

Consolidation and centralization improves efficiency and reduces operational costs. But narrowly focusing on cost-cutting ignores the potentially dangerous threat to system security if consolidation ignores the perils of monoculture, reduction in redundancy and surge capacity, and the effects of self-organization. Complexity theory considerations reveal the negative side of consolidation—self-organized monoculture systems with giant hubs promote the spread of malware and increase the likelihood of total collapse. Concentration and homogenization of critical assets, elimination of redundancy and surge capacity, and tightly coupled systems result in vulnerabilities not typically considered by policymakers.

When consolidating and centralizing to save money, system designers and administrators need to take special precautions to offset the downside of centralization and standardization with extra vulnerability-reducing precautions. This typically means that hardware and software systems and communication networks must be hardened even more against accidental and deliberate attacks. That is, vulnerability must be reduced to compensate for the increase in self-organization. Mathematically, this means vulnerability (v) must be reduced to offset spectral radius (r).

B. RECOMMENDATIONS

Making the assumption that we cannot mitigate every possible threat, hazard, or vulnerability, we should focus on resilience. According to DHS, resilience means the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[135] But efficient systems carry inherent vulnerabilities, so how do we balance efficiency and resiliency to ensure system security? Since resilience of a system is proportional to the relationship between vulnerability and spectral radius (vr), any

[135] DHS Risk Steering Committee, *Risk Lexicon*.

increase in v, r, or both decreases resilience.[136] Specifically, in the examples given in Figures 3 and 4, for a given v, r increases from 3.03 to 4.0 as consolidation and centralization in the data center becomes a hub-and-spoke network, as illustrated by Figure 4. Assuming all other factors are equal, centralization reduces resilience. The central data center hub is a single point of failure.

As discussed previously and shown in Figure 5, vulnerability is counter-proportional to resilience. So a reduction in overall vulnerability can compensate for increased self-organization and loss of resilience. We can balance risk and resilience by noting that resilience after centralization can be less than or equal to resilience before centralization by lowering vulnerability, v, as follows:

$$v(\text{data center})\, r(\text{data center}) \leq v(\text{before consolidation})\, r(\text{before consolidation})$$

substituting r(before consolidation) = 3.03, r(data center after) = 4, and dividing:

$$v(\text{data center}) = 3.03\, v(\text{before})/4.0\, v(\text{after}).$$

In this example, a 25-percent reduction in vulnerability will compensate for the resilience lost due to centralization. Vulnerabilities in an enterprise system can be the result of a variety of issues, including design flaws in software or hardware and organizational policy weaknesses. A list of typical vulnerabilities in enterprise systems and countermeasures, which reduce vulnerability, follows in Table 6.

[136] Lewis, *Critical Infrastructure Protection*, 65.

Table 6. Typical Enterprise System Vulnerabilities and Countermeasures[137]

Vulnerability	**Countermeasure**
Power failure	Install backup power supply
Telecom failure	Buy redundant telecom service
SYN attack	Install IDS; install firewall: filter ports
No IDS	Install IDS
Break-In	Install IDS; install firewall: filter ports; install latest patches
Clear password file	Encrypt password files
No backup	Conduct periodic backups
No firewall filter	Install firewall: filter ports
No antivirus	Install antivirus and patches
Clear XML/HTML	Install HTTPS/SSL; install PKI/VPN
Weak encryption	Install 3DES or AES; install PKI
Password not changed	Change password periodically
War dialing	Close modem ports
Weak LDAP in applications	Install LDAP directory; modify applications
Buffer overflow	Install patches; update patches
Weak OS patches	Update patches; install IDS; install firewall: filter ports
Open Wi-Fi ports	Install IDS; install firewall: filter ports; encrypt Wi-Fi sessions; authenticate Wi-Fi users
Open modem	Close dial-up modems or use VPN
Open FTP ports	Close FTP or filter ports
Firewall filter off	Turn on firewall filtering

[137] Adapted from Lewis, 159.

Based upon previously identified areas of vulnerability in cloud computing, in addition to requiring strong security protocols, organizations should pay close attention to account configurations in order to avoid simple mistakes that lead to large consequences. Organizations should also consider the consequences of hosting applications, data, and infrastructure in the cloud and deciding which of these require redundancy and failover capabilities. It may not be cost-effective to store highly sensitive or important data in a public cloud if the consequences of loss or the inability to access the data require on-premises backup and failover. For centralized, government IT organizations, it may be just as cost-effective to host an on-premises cloud that provides service to all government agencies, with redundancy at a backup data center.

Redundancy may help increase robustness against attack or component hardware failure. For instance, a power failure at a data center can be mitigated through backup generators. The consequences of a catastrophic incident at a data center can be mitigated through the existence of a backup data center in another location, including cloud services provided by a third party. Consequences from the loss of a server due to hardware or software failure can be mitigated through a backup server and automated failover. However, the cause of the failure may be a weakness in the backup as well when the units are the same. Similarly, a vulnerability to an attack or exploit that exists in one device or software application will exist in any backup as well.

To mitigate vulnerabilities due to monoculture, introduce diversity. This practice is already in place in some of the most critical infrastructure in the country—commercial nuclear reactors.[138] The Nuclear Regulatory Commission recognizes that even the best quality assurance does not adequately prevent common mode failures when redundant systems are of the same hardware and software. Designed-in diversity is used for commercial nuclear reactor safety in order to avoid common defects and weaknesses in redundant systems. If redundant systems are substantially different from one another, a

138 "Diversity and Defense in Depth in Digital Instrumentation and Controls," United States Nuclear Regulatory Commission, accessed February 6, 2018, https://www.nrc.gov/about-nrc/regulatory/research/digital/key-issues/diversity-defense.html.

failure in one will not necessarily mean a failure in the other.[139] This obviously comes at a cost, but it is critical to ensuring resilience of the system. However, organizations can evaluate which applications and components are most vulnerable and invest specifically in those areas. Focusing on areas that will have the most impact minimizes additional costs but, most importantly, reduces the likelihood of a catastrophic failure that disables the entire system due to malware and makes it more difficult for attackers.

As previously discussed, SOC is measured by spectral radius, which increases as link density and hub size increase. To mitigate for this, organizations can reduce the size of hubs and concentration of links, thereby increasing resiliency. Operating systems inefficiently will keep them from becoming critical.[140] Concentration of assets, such as consolidated data centers and other infrastructure, can result in single points of failure. Redundancy, such as a backup data center, can increase system robustness against a physical attack.[141] Organizations will have to carefully weigh this against the fact that the high connectivity may result in decreased resiliency against cascade failures.[142]

We cannot mitigate every possible threat, hazard, or vulnerability and should focus on actions that will increase resilience, several of which have been proposed here. There is a cost to many of the proposed solutions, but they are flexible enough to allow organizations to determine the tradeoffs they are willing to make between efficiency and security.

---

139 R. H. Wyman and G. L. Johnson, "Defense against Common-Mode Failures in Protection System Design" (report, Lawrence Livermore National Lab, 1997), 249, http://inis.iaea.org/Search/search.aspx?orig_q=RN:30053658.

140 Lewis, Mackin, and Darken, "Critical Infrastructure," 10.

141 Lewis, *Critical Infrastructure Protection*, 60.

142 Lewis, 60.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bak, Per. *How Nature Works: The Science of Self-Organized Criticality*. New York: Copernicus, 1996.

Bak, Per, Chao Tang, and Kurt Wiesenfeld. "Self-Organized Criticality: An Explanation of 1/f Noise." *Physical Review Letters* 59, no. 4 (July 27, 1987): 381–4.

Barabasi, A. L. "The Architecture of Complexity." *IEEE Control Systems* 27, no. 4 (August 2007): 33–42. https://doi.org/10.1109/MCS.2007.384127.

Bayard, Madeleine, and Erin Lee. "Review of State Information Technology Consolidation Efforts." Issue brief, NGA Center for Best Practices, 2005. https://www.nga.org/files/live/sites/NGA/files/pdf/0512Consolidationissuebrief.pdf.

Bertuglia, Cristoforo Sergio, and Franco Vaio. *Nonlinearity, Chaos & Complexity: The Dynamics of Natural and Social Systems.* New York: Oxford University Press, 2005.

Birman, Kenneth P., and Fred B. Schneider. "The Monoculture Risk Put into Context." *IEEE Security & Privacy* 7, no. 1 (February 2009): 14–17. https://doi.org/10.1109/MSP.2009.24.

Brown, Kathi Ann. *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. Fairfax, VA: Spectrum Publishing Group, 2006.

Burke, Dennis. "All Circuits Are Busy Now: The 1990 AT&T Long Distance Network Collapse." Paper, California Polytechnic State University, 1995. http://users.csc.calpoly.edu/~jdalbey/SWE/Papers/att_collapse.html.

Deloitte. "IT Transformation Future State Enterprise Architecture Strategy." Report, State of Illinois, 2016.

———. "State of Illinois Current State Assessment." Report, State of Illinois, 2016. https://www2.illinois.gov/sites/doit/Strategy/Transformation/ProgramWiki/Documents/CurrentStateAssessment.pdf.

———."State of Illinois—IT Transformation Future State Recommendations." Report, State of Illinois, 2016.

Demchak, Chris C. "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)." *Journal of Comparative Policy Analysis: Research and Practice* 14, no. 3 (2012): 254–69. https://doi.org/10.1080/13876988.2012.687619.

Department of Defense. *2014 Quadrennial Defense Review*. Washington, DC: Department of Defense, 2014. https://www.defense.gov/Portals/1/features/defenseReviews/QDR/2014_Quadrennial_Defense_Review.pdf.

Department of Homeland Security. *Information Technology Sector-Specific Plan: An Annex to the NIPP 2013*. Washington, DC: Department of Homeland Security, 2016. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf.

Department of Homeland Security Risk Steering Committee. *DHS Risk Lexicon: 2010 Edition*. Washington, DC: Department of Homeland Security, 2010. https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

Government Accountability Office. *Data Center Consolidation Agencies Making Progress, but Planned Savings Goals Need to Be Established*. GAO-16-323. Washington, DC: GAO, 2016. https://www.gao.gov/assets/680/675592.pdf.

Grobauer, Bernd, Elmar Stocker, and Tobias Walloschek. "Understanding Cloud Computing Vulnerabilities." *IEEE Security & Privacy* 9, no. 2 (April 2011): 50–7.

Huaxia, Zhang. "Exploring Dynamics of Emergence." *Systems Research & Behavioral Science* 24, no. 4 (July 2007): 431–43, https://doi.org/10.1002/sres.

Illinois Office of the Secretary of State. *Executive Order Consolidating Multiple Information Technology Functions into a Single Department of Innovation and Technology*. Illinois Executive Order 2016-01. Springfield, IL: Senate of Illinois Executive Department, 2016. https://www2.illinois.gov/Documents/ExecOrders/2016/ExecutiveOrder2016-01.pdf.

Illinois State Board of Elections. "Illinois Voter Registration System Database Breach Report." Report, Illinois State Board of Elections, 2016. www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_26_16AgendaAmended.pdf.

Institute for Critical Infrastructure Technology. "Handing Over the Keys to the Castle. OPM Demonstrated That Antiquated Security Practices Harm National Security." Report, Institute for Critical Infrastructure Technology, 2015. http://icitech.org/wp-content/uploads/2015/07/ICIT-Brief-OPM-Breach2.pdf.

Jansen, Wayne, and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing*. Special Publication 800-144. Gaithersburg, MD: NIST, 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

Kennel, David. *OPM vs. APT: How Proper Implementation of Key Controls Could Have Prevented a Disaster*. North Bethesda, MD: The Sans Institute, 2016. https://www.sans.org/reading-room/whitepapers/breaches/opm-vs-apt-proper-implementation-key-controls-prevented-disaster-36852.

Kissel, Richard (Ed.). *Glossary of Key Information Security Terms*. NISTIR 7298 Revision 2. Gaithersburg, MD: NIST, 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Lala, Jaynarayan. "IT Monoculture Security Risks and Defenses." *IEEE Security & Privacy* 7, no.1 (2009): 12–13.

Lewis, Ted G. *Bak's Sandpile: Strategies for a Catastrophic World*, Kindle edition. Williams, CA: Agile Press, 2011.

———. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, 2nd edition. Hoboken, NJ: John Wiley & Sons, 2015.

Lewis, Ted G., Thomas J. Mackin, and Rudy Darken. "Critical Infrastructure as Complex Emergent Systems." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 1 (January–March 2011): 1–12. http://dx.doi.org/10.4018%2Fijcwt.2011010101.

Mell, Peter, and Timothy Grance. *The NIST Definition of Cloud Computing*. Special Publication 800-145. Gaithersburg, MD: NIST, 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Paczuski, Maya, and Per Bak. "Self-Organization of Complex Systems." Cornell University Library, June 5, 1999. http://arxiv.org/abs/cond-mat/9906077.

Partnership for Public Service. *Helping Government Deliver II: The Obstacles and Opportunities Surrounding Shared Services*. Arlington, VA: Deloitte, 2015. https://www.govexec.com/media/gbc/docs/pdfs_edit/031315cc1.pdf.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press, 1984.

President of the United States. *Critical Infrastructure Security and Resilience*, PPD-21. Washington, DC, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Rickles, Dean, Penelope Hawe, and Alan Shiell. "A Simple Guide to Chaos and Complexity." *Journal of Epidemiology and Community Health* 61, no. 11 (November 2007): 934. https://doi.org/10.1136/jech.2006.054254.

Williams, Daniel, Wei Hu, Jack Davidson, Jason Hiser, John C. Knight, and Anh Nguyen-Tuong. "Security through Diversity: Leveraging Virtual Machine Technology." *IEEE Security & Privacy* 7, no. 1 (2009): 26.

Wyman, R. H., and G. L. Johnson. “Defense against Common-Mode Failures in Protection System Design.” Report, Lawrence Livermore National Lab, 1997. http://inis.iaea.org/Search/search.aspx?orig_q=RN:30053658.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California