



Calhoun: The NPS Institutional Archive
DSpace Repository

Center for Homeland Defense and Security (CHDS)

Homeland Security Affairs (Journal)

2017

Homeland Security Affairs Journal, Volume 13 / 2017 UAPI Summit Special Issue

Monterey, California. Naval Postgraduate School, Center for Homeland Defense and Security

<http://hdl.handle.net/10945/57820>

The copyright of all articles published in Homeland Security Affairs rests with the author[s] of the articles. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. Anyone can copy, distribute, or reuse these articles as long as the author and original source are properly cited.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



Homeland Security Affairs

Volume 13 / 2017

UAPI Summit Special Issue

Director's Introduction to the UAPI Summit Special Issue

The University and Agency Partnership Initiative (UAPI) is a cornerstone element of the CHDS mission of serving as “the Nation’s Homeland Security Educator.” Its mission: facilitate educational collaboration among institutions and agencies to support development of academic programs that enable a professional workforce and promote critical thinking in homeland security. The Initiative’s primary outcome is a sustainable network of university partners delivering the highest quality academic experience for students in homeland security and related fields. Leveraging CHDS materials and expertise, UAPI provides support to partners launching homeland security programs, helps prevent redundancy in curriculum development, and encourages partners to improve and add to the curricula that already exists.

In addition, UAPI organizes national and regional events that enable cross-institutional information exchange and encourage practitioner engagement with the broad capabilities of academia. The 10th Anniversary Homeland Defense & Security Education Summit, held in March 2017 in partnership with the DHS Office of Policy and hosted by George Mason University, is the premier example of UAPI’s effort to connect people and ideas. The outstanding papers that comprise this special issue of Homeland Security Affairs represent a sample of the depth and purpose of research across the Homeland Security enterprise. Readers might find value in these essays on two levels: first, in the theses proposed and the quality of the papers themselves; as well, I hope that the sample research provided here will stimulate interest in further engaging the remarkable capabilities across our community. On behalf of UAPI and our partners, thank you, and enjoy this special issue!

Steve Recca, Director, University and Agency Partnership Initiative

Notes from the Editor

For the 2017 UAPI Summit Special Issue, *Homeland Security Affairs* presents the best papers from the 2017 University and Agency Partnership Initiative (UAPI) Summit Conference. This issue also contains executive summaries from eleven other outstanding papers from the UAPI Summit. All of the papers submitted for presentation at the meeting were vetted by an academic jury, and then the five best papers were selected by the *Homeland Security Affairs* Editorial Committee.

In [“Cyber Border Security—Defining and Defending a National Cyber-Border,”](#) Phillip Osborn explores the concept of a cyber-border and explains how it can be applied and defended in the field of cyber-security.

In [“Applying an Organizational Framework to Examine Jihadi Organizations as an Industry,”](#) Michael Logan, Gina Ligon, and Douglas Derrick apply an organizational and industrial psychology approach to ascertain how certain characteristics of terrorist groups affect their performance.

In [“Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs,”](#) Duane Verner, Frederic Petit, and Kibek Kim, present an algorithm-based approach for identifying the most critical nodes in a critical infrastructure system.

In [“A Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, Resilience and ‘Anti-Fragility,’”](#) Eric Taquechel and Ted Lewis build on their previous work in applying insights from network science, operations research, complexity theory, and cognitive psychology to create a better approach to measuring risk and leveraging deterrence in critical infrastructure protection.

In [“The Roots of Community Resilience: A Comparative Analysis of Structural Change in Four Gulf Coast Hurricane Response Networks,”](#) Thomas Haase, Gunes Ertan, and Louise Comfort examine whether investments in information technology influenced the structural development and evolution of four disaster operations networks that formed in response to hurricanes in Louisiana and Texas.

An aerial night photograph of a city, showing a dense network of glowing yellow and orange lights against a dark, textured background. The lights form a complex, branching pattern across the lower two-thirds of the image, suggesting a city's infrastructure or a network of data. The top third of the image is a solid dark band where the title is placed.

Cyber Border Security – Defining and Defending a National Cyber Border

By Phillip Osborn

Abstract

Concerns stemming from the convergence of border and cyber security threats are nothing new to those involved in both disciplines. Criminals and foreign actors have been exploiting computers and cyber methods to circumvent physical border security for decades. Today nearly every crime or homeland security threat that once required some physical nexus with the nation's traditional borders (land, sea, and air) is being committed, or at least facilitated, by some cyber component. In many ways vulnerabilities in cyber security render some aspects of traditional border security irrelevant, or at the very least, much less secure. The article explores this convergence of traditional border and cyber security and proposes a policy that would seek to evolve the concept of border security to include the cyber domain. Based on policy work begun over a decade ago by the author while the national cybercrime program manager for the U.S. Customs Service, the article details how a national cyber border can be defined and enforced. Relying on a methodology that adapts existing authorities, the article provides logical justifications and arguments for the need and legal authority to define a national cyber border. The strengths and shortcomings of this adaptive methodology are explored along with issues which may require new legislation. The article addresses some of the privacy concerns which are certain to arise from the cyber border concept using the same adaptive methodology of existing protections and expectations of privacy. The ultimate goal of the article is to stimulate thought-provoking discussion and spur further academic research into the convergence of cyber and border security; issues which are interdependent and clearly in the forefront of homeland and national security.

Suggested Citation

Osborn, Phillip. "Cyber Border Security – Defining and Defending a National Cyber Border." *Homeland Security Affairs* 13, Article 5 (October 2017). <https://www.hsaj.org/articles/14093>

Introduction

While the protection and control of our national borders has always been an important issue, the emergence of terrorist threats over the past several decades has brought concerns over border security to the forefront of national and homeland security discourse. A major topic in the 2016 presidential election contest, increasing border security became the central theme of the eventual victor and perhaps a strong indicator of the importance of the issue to a large portion of the electorate. Another less traditional security concern, but one that has rung alarms around the world, is the issue of cyber threats. Because of their asymmetrical nature and potential severity, cyber threats have become an overarching subject to national and homeland security interests. This document asserts that the two-- border threats and cyber threats-- are not mutually exclusive, and it explores the convergence of border and cyber security. Further, this article will show that the evolution of the concept of the border beyond the traditional land, sea, and air frontiers of the nation to include the cyber border is both inevitable and necessary. The article outlines the justification and conceptual framework for defining a national cyber border based on historical and traditional border analogies, and will discuss the existing legal framework that makes defining a national cyber

border possible, along with the authorities for protecting it. The purpose of this discussion is to introduce what at first may seem an exotic concept, and then to bring greater clarity and understanding of the subject to the researcher or homeland security professional. The article primarily focuses on defining the legal justifications for enforcing a national cyber border through the adaptation and interpretation of current and traditional U.S. border enforcement authorities. It leaves much of the “how” of policing it to the further academic and legal research that it hopes to stimulate. The following analogy is offered as food-for-thought regarding the cyber border and the debate for which this document hopes to be the catalyst. For hundreds of years, the distance of a cannonball shot was used to measure how far from shore a country should extend its legal control and territorial claims.¹ Leaders arrived at this distance based on the best technology of their day-- a cannon shot. This distance has changed and evolved over the years as newer technology made this original metric obsolete. We owe the founders of our country and the people of the nation our best attempt at interpreting the technologies of our day to develop policies and strategies to address the dynamic ways that cyberspace is changing the world and impacting national security.

The Convergence of Cyber and Border

What is border security and why is it so important? Simply put, the border is the point where foreign threats become domestic realities. The right and duty of government, is to control who and what crosses the nation’s borders to protect the country and its people from foreign threats. The threats range from the obvious such as terrorists or criminals seeking to perpetrate an attack or commit a crime, to the less obvious such as contaminated agricultural and food products which could severely impact the nation’s farming industry or sicken the populous. Because protection of the nation is such a compelling interest, border security is clearly viewed as a primary responsibility of the state. The traditional border security efforts of the government are obvious. Customs and Border Protection officers, Border Patrol Agents, and Coast Guard cutters are all physical measures employed to control the movement of persons and material entering, and in some cases exiting the country. These measures are a series of physical deterrents and inspection capabilities at the nation’s boundaries to identify and control who and what is allowed to cross the border. The emergence of cyber threats however has radically changed the border security landscape forever.

The Internet and cyber methods provide an opportunity to circumvent traditional border security measures to perpetrate crimes and to harm the nation to a degree once only possible through large scale military actions. Terrorists, criminals, and nation states can and do take advantage of the asymmetrical nature of cyber methods to threaten and harm the nation and its people. Attacks on critical national infrastructure, the theft of sensitive government and industry trade secrets, the importation of hazardous and illegal materials, and the stealing of funds from banks and citizens are just a few of the crimes and threats that once normally required some physical compromise of traditional border security and controls to perpetrate. All of these actions are now possible by the illicit use of the Internet. Some crimes commonly committed against individuals by foreign actors today, like the theft of personal information or finances, would have been impossible or improbable before the advent of the new “cyber vector” of attack. Today cyber threats have converged with traditional border security threats and now either complement them, or provide new

opportunities to threaten the nation. By providing an avenue to circumvent physical border security measures, cyber methods have made many traditional border security efforts obsolete.

The Need to Define the Nation's Cyber Border

With cyber threats being such an obvious danger, one would assume that the government would take a similar responsible role in protecting the nation from foreign intrusions and threats, however this is not the case. Unlike traditional border security, the government's role in defending the nation from foreign cyber intrusion is far less robust. Rather than focusing on preventing the entry of cyber threats, the government functions in a response role, investigating after the fact and after an attack has occurred. Defense of the nation's cyber frontier is largely left up to private entities, both persons and organizations, to protect their own cyber borders. From a border security perspective this is highly undesirable due to interdependency issues since each individual or organization's computer or network once compromised can become an additional attack vector operating within the borders of our nation. This situation is analogous to making every individual responsible for their own physical border security, and ultimately that of the entire nation. Imagine the government conceding responsibility for land border security to the private land owners living along the border with little more than recommended best practices and advice on protecting their portion of the border. Imagine the responsibility for food and drug safety being left up to the individual consumers or businesses importing these goods. While this may sound absurd, this is essentially the situation in the government's approach to cyber threats.

One solution to the problem of foreign cyber threats is the evolution of the concept of the cyber border. Once the concept of cyber border is defined, the government can use traditional laws and authorities to better protect the nation from current and future foreign cyber threats.

Borders in Cyberspace

An oft-repeated line is that in cyberspace there are no borders. This statement, while philosophically desirable among those seeking a more open world and society, is simply not true. There are physical borders that data transmission lines cross and there are functional equivalents of the border where data arrives directly from foreign places-- a very important concept that will be discussed further. The concept of borders in cyberspace even permeates computer network phraseology where terms such as "border routers" and "demarcation lines" are used to express the boundaries between networks. Yes, there are borders in cyberspace, we have just chosen not to acknowledge the cyber border as we do the land, sea, and air borders. Disruptive technologies which impact traditional border concepts are nothing new; the Internet is just the most recent. Air transport was another disruptive technology which required an evolution in traditional border security thinking and which provides an easy analogy to justify a similar evolution in the concept of the cyber border.

Disruptive Technologies and Border Security

The advent of air travel could arguably be judged as equal to or exceeding the Internet in the disruptive impact it has had on the world. Like the Internet, it has opened up opportunities for commerce and contact between peoples that would otherwise not exist. Like the Internet, air transport has also had a major impact on how war is waged, In terms of border security impact, air travel was also disruptive since there was no longer a traditional land or sea crossing at the countries' boundaries. Aircraft could fly across the borders and land deep within the country. The response to this was not to surrender border security and authority over what and who was entering the country via aircraft, but an adaptation and evolution in the definition of the border which allowed the exercising of traditional border authorities. The definition of the cyber border requires a similar adaptation and evolution in border thinking.

Defining the Cyber Border

Many current legal rulings and decisions regarding the Internet and Cyberspace are based on the interpretation of existing laws that govern conventional non-cyber circumstances. In many cases this methodology has succeeded in finding a workable application of existing laws, while in others, attempts at such an application have been cumbersome. Viewed in this light, the governance of cyberspace and the Internet may ultimately require some radical departure from contemporary legal thinking, perhaps a new separate U.S. Code crafted specifically for it. However, the legal framework to define the cyber border appears to be already present without any modifications or additions to existing laws.

Traditional Borders

The concept of traditional border— land, sea, or air—is relatively easy to grasp. Land borders are the geographic boundary separating the adjacent territories of other countries. The sea borders are a bit more complex and extend the physical border seaward from shore out to a specified distance. Currently this distance is 12 nautical miles seaward from the U.S. coast, increased from a 3 nautical distance which had been the distance claimed for many years. This claimed 12 mile zone is referred to as the territorial sea and is treated as the maritime border of the country. Additionally, the U.S. claims a further 12 mile nautical distance from the boundary of the territorial sea as Customs waters effectively allowing enforcement of customs and border controls seaward 24 nautical miles from the U.S. coast. Further, the U.S. claims an additional 200 mile seaward zone to enforce an economic, exploratory and exploitation zone which evolved from a 200 mile fishery conservation zone.² The variations and adjustments to border enforcement in the maritime realm are pragmatic and reflect the reality that time and technology necessitate changes and adaptations in order effectively to protect the nation. A similar adaptive view concerning enforcement of the air border discussed next, can also be used to define the cyber border.

The Air Border Analogy

The air borders are simply vertical extensions of the land and sea borders allowing control of the nation's airspace. As an aircraft enters U.S. airspace it is very much crossing the nation's border. Performing a Customs inspection of the aircraft, its passengers, and its cargo however would obviously be impractical at 35,000 feet. Where the aircraft lands therefore becomes what is referred to as the Functional Equivalent of the Border or FEB. The FEB is the first practical point where border controls can be exercised on the aircraft.³ The clearest example of FEBs would be the foreign arrival areas of international airports where immigration and customs inspections of aircraft, passengers, and cargo are conducted well away from the actual physical border at its functional equivalent.

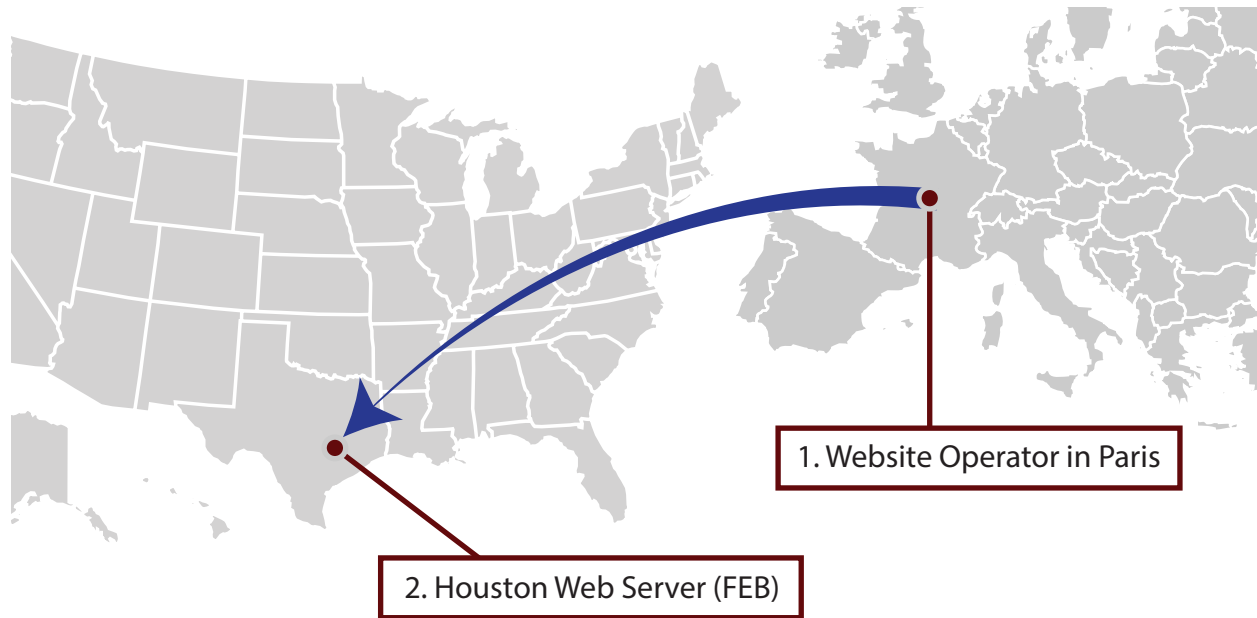
Functional Equivalents of the Border

The concept of the Functional Equivalent of the Border (FEB) is critical to border security because it allows the legal imposition of regulatory requirements (search, inspection, and seizure) away from the physical borders. In order to have an FEB, circumstances must exist which create the same environment as the border: those being: 1) there is a "nexus" to the border, a border crossing, or to something which has crossed the border; 2) there is a reasonable certainty that there has been no material change since the nexus with the border; and 3) the search and/or inspection occurs at the first practical detention point after the border crossing.⁴ It is this same type of interpretation of the FEB that makes defining the cyber border largely possible.

The Cyber Border

The simplest method to define the cyber border is to apply the land border concept. The place where data transmission cables cross the physical national borders would constitute a border crossing. This analogy is deficient, however, since data can cross the border via other means independent of terrestrial data transmission cables – via satellite for example. It is also impractical for border protection and inspection for the same reason inspection of an in-bound aircraft at 35,000 feet is impractical. The cyber border therefore is best defined as the FEB where the data arrives at the first practical point of inspection— a network router, computer server, PC, or other networked device.

The web site example depicted in figure1 demonstrates the FEB concept applied to the cyber border. It depicts a World Wide Web (www) site involved in the sale of some type of illegal merchandise. This merchandise could be any item that would constitute an illegal import at the border such as controlled substances, counterfeit products, or child pornography. In this example the web site is hosted on a server located in the U.S., but directly managed and controlled by a foreign located criminal.

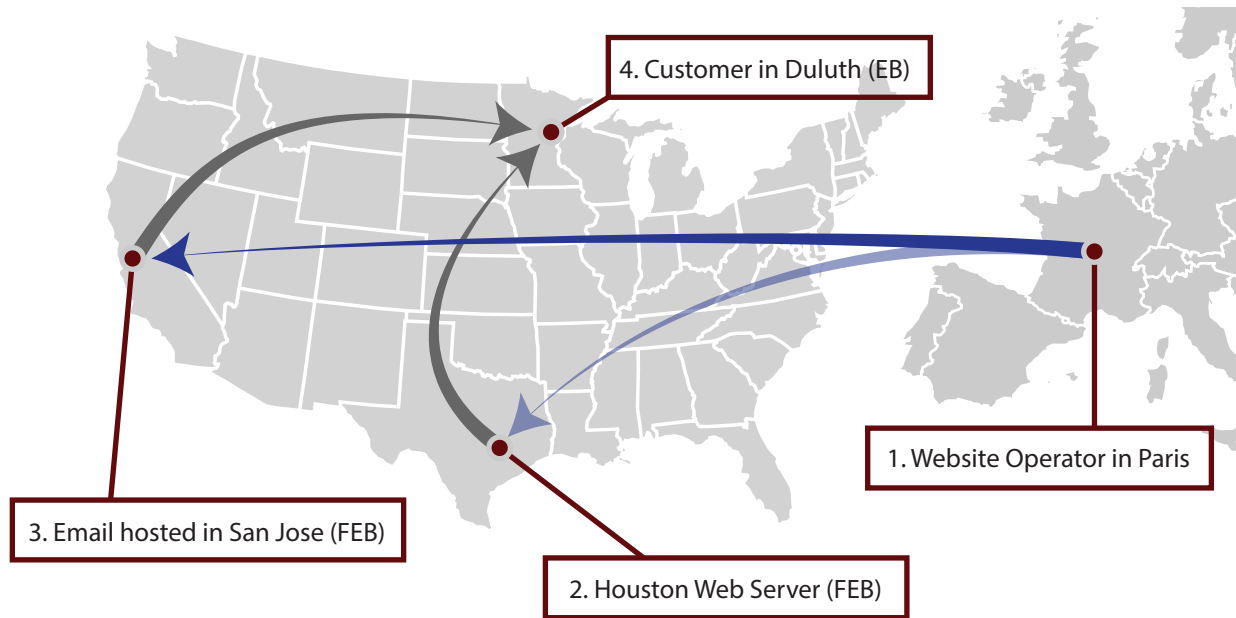


The website operator in Paris (1) logs into their web hosting account in Houston (2) and uploads merchandise (software, music, movies, etc.) that is advertised for sale and download from their web site. The Houston web server becomes a Functional Equivalent of the Border (FEB).

Figure 1. Example of direct delivery of merchandise from a foreign entity

The illicit web site in the example above could be providing information on the merchandise for sale, how to place an order, how to pay for the merchandise, and the options to arrange delivery. In the case of Internet deliverable merchandise, the web site can also be the point where customers access and retrieve (download) the merchandise; alternately the customers could also be directed to a second web site or file server to download the merchandise. Still another option is it that the customer can receive the merchandise directly as an email attachment from the seller from either a foreign or domestic email server.

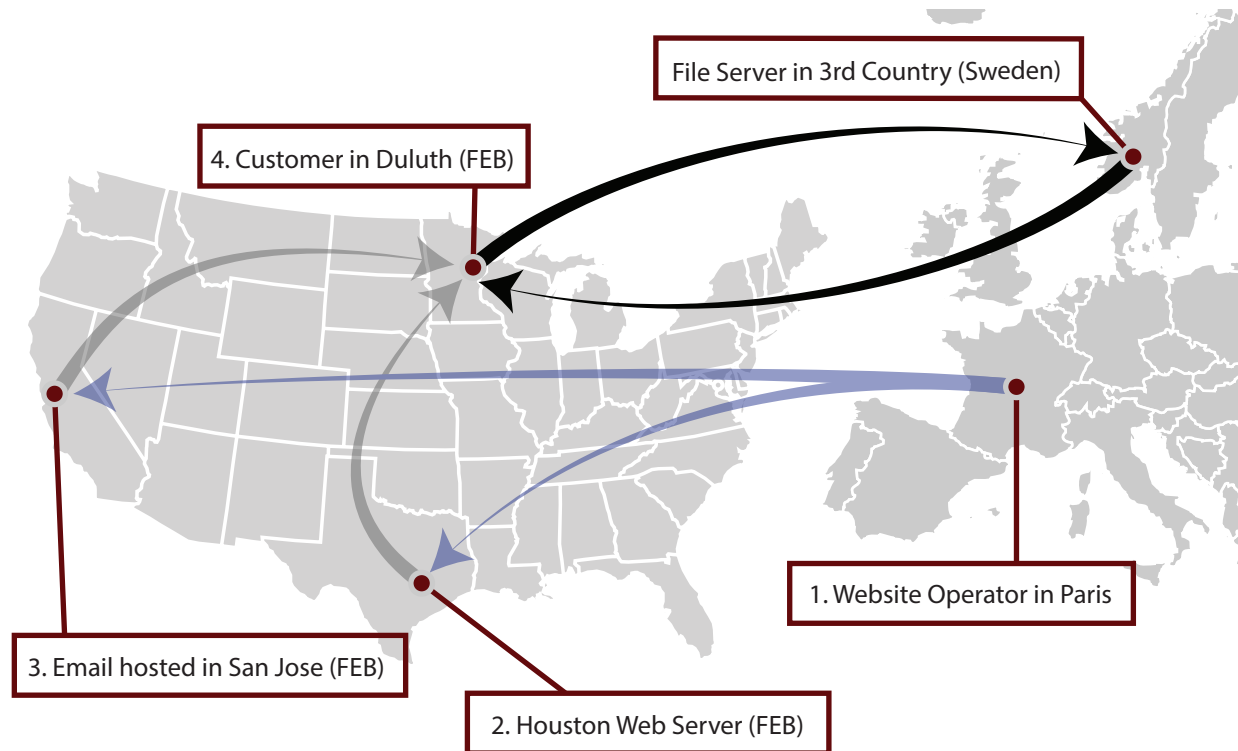
Figures 2 and 3 depict more complex scenarios for an illicit web site that involves the interpretation of multiple FEBs involved in the ordering and receipt of illegal imports.



3. The website operator in Paris receives customer orders and sends invoices and download instruction to customers via their email account hosted in San Jose which becomes a Functional Equivalent of the Border (FEB).

4. A customer in Duluth sends an order for merchandise via email to the seller's email account hosted in San Jose and receives the order invoice and the download instructions from the seller. The customer then downloads the merchandise from the seller's website in Houston directly to the customer's computer which becomes and Extended Border (EB).

Figure 2. Example of direct delivery of merchandise from a foreign entity with multiple FEBs



4. Customer accesses seller's file server in third country (in this example Sweden) and downloads the merchandise directly to their computer. The customer's computer effectively becomes a Functional Equivalent of the Border (FEB).

Figure 3. Another example of direct delivery of merchandise from a foreign entity with multiple FEBs

Critical to the understanding of how the FEB concept applies to defining the cyber border is an understanding of border enforcement authorities and how they work to protect the nation from border threats, while also addressing important constitutional and privacy concerns.

Border Search Authorities and Their Application to the Cyber Border

One of the most important border protection tools is the border search authority. This long-standing authority held by Customs officers and other authorized officials dates from the time of the nation's founding and is derived from some of the first statutes passed by Congress.⁵ Based on Congress's broad authority to regulate foreign commerce and enforce immigration laws, border search authority is a long-established exception to the Fourth Amendment's probable cause and search warrant requirements.⁶

The contemporary threat from terrorism and a basic interest in national self-protection make border search authority a necessary and legally accepted exception to normal 4th Amendment concerns. Border search authority allows for the warrant-less inbound and outbound search of persons, conveyances, and merchandise at the borders, the functional equivalent of the border, and in some other cases away from the border at what is referred to as the extended border.⁷ While traditional border searches focus on the inspection of people, conveyances, and merchandise, the focus of cyber border searches would focus on the import and export of digital merchandise.

The primary purpose of a Customs border search is to inspect persons, baggage, and merchandise to ensure that duties are collected and to ensure that whatever is entering or leaving the country is in compliance with U.S. law.⁸ Another important purpose of these searches is to search for and seize prohibited imported or exported merchandise. The definition of merchandise is “goods, wares, and chattels of every description.”⁹ If there is any debate as to whether the data carried over the Internet is merchandise it would come as a surprise to the thousands of copyright owners and vendors of software, music, movies, and books which are delivered to millions of customers daily via the Internet, or to the customers who pay for this digital merchandise. The debate on whether digital data is imported or exported in the traditional sense can be argued as being a function of the origin and ultimate arrival country of the digital merchandise. The illegal material or contraband which can be and is imported and exported via the Internet runs the gamut from child pornography, to counterfeit or illegally copied software and music, to stolen credit card information, to seditious materials— all materials which would be subject to seizure as imports or exports contrary to law.¹⁰

Of special importance to the cyber border discussion, particularly in the area of border inspection, is the inclusion of documents within the purview of a border search.¹¹ As stated previously, web sites advertising the sale of some type of merchandise can be simply that, an advertisement for a product, which provides a channel for the customer to contact and arrange the purchase and delivery of the merchandise. These contacts and arrangements can be accomplished through a variety of avenues including via email, web messages, or via an advertised telephone number on the web site. In the case of a web site being controlled by a foreign source, the email associated with the web page will likely contain information relating to the orders for these products and services and should be considered as documents relating to the importation of the merchandise. In the illustration examples, the emailed documents pertaining to orders from customers, whether those customers are located in the U.S. or elsewhere, are retrieved by the foreign source from a domestically located U.S. email or web server and transferred/exported to their foreign source’s location. Conversely, documents relating to the orders sent from the foreign source to customers in the U.S. are sent from the foreign source’s computer and are imported to their email server located in the U.S. In a traditional border search scenario, documents arriving from a foreign source, whether carried on a person, in baggage, or accompanying the merchandise, would be subject to search and examination to see if they pertained to the importation of goods. These same documents arriving via the Internet are not subject to this same search.

A domestically hosted but foreign-manipulated web site can not only serve as simply an advertising and ordering mechanism for merchandise that is shipped via traditional parcel service or mail, but can also serve as the actual delivery vehicle for the merchandise. Web sites that offer digital merchandise such as software, music, and videos commonly store the merchandise in separate file directories on the web host computers that the customers pay

to access. In such cases it is reasonable to assume that the digital merchandise placed in these file directories by the foreign source was imported to those computers by the foreign source from their foreign location. In most cases this can be verified by inspecting the IP history logs maintained by the web hosting company. The digital merchandise located on a domestic web hosting company computer/server that has been imported to that computer/server by a foreign web site operator should be subject to a Customs border search as an FEB.

Legal Merchandise versus Prohibited Merchandise

The Internet border search issue goes well beyond just the concern of illegal imports and contraband, but also to the much wider subject of general merchandise being imported via or assisted by the Internet. The exponential growth of Internet e-commerce represents legitimate commerce by both individual consumers and corporations. Internet border search authority may eventually be required to fulfill the other Customs missions of protecting the nation's revenues and for the proper assessment of duties. While the immediate impact that the addition of Internet/cyber border authorities would be most evident in the suppression of smuggling and other illegal activities, the benefit to the overall revenue protection may eventually prove just as significant.

Merchandise versus Communications

Current border search authority allows authorized officials to search for imported or exported merchandise including documents, at the border or its functional equivalent. This discussion of redefining the border for the purposes of enforcing a cyber border is not directed at private communications unless those communications pertain to an importation or exportation of merchandise— legal or otherwise.

Privacy Issues and Concerns

The cyber environment should not enjoy any enhanced protections over what persons should rightfully expect in the traditional physical world. Therefore, privacy issues involving the cyber border should be of no greater concern than in a traditional border situation. Since the focus of cyber border enforcement is on merchandise (legal and illegal, entering or exiting via the cyber border), private or privileged communications are already protected from inspection the same as in non-border situations.¹² Only data containing merchandise or documents relating the import/export of merchandise, legal and illegal, would be subject to inspection and border search and seizure. Granted, the cyber world does present some issues which may not have a corollary in the non-cyber world, but just as the evolved view of the traditional border must be adapted, so must the interpretation of border authorities so they may evolve to address the uniqueness of the cyber environment.

Conclusion

The importance of defending the nation against cyber threats is critical to national and homeland security. The magnitude of current and emerging cyber threats is equal to and may in actuality surpass traditional threats. The asymmetrical nature of cyber provides to minor nation-state enemies and even lone wolf actors the ability to inflict great harm to a great military power like the United States. Criminals do and will continue to exploit cyber to their advantage rendering many aspects of traditional crime prevention ineffective or obsolete. Stopping and preventing foreign threats at the border has been and always will be a key element in protecting the nation and its people. Adapting and evolving our definition of the border to define a national cyber border will help deny this pathway for foreign threats into our country.

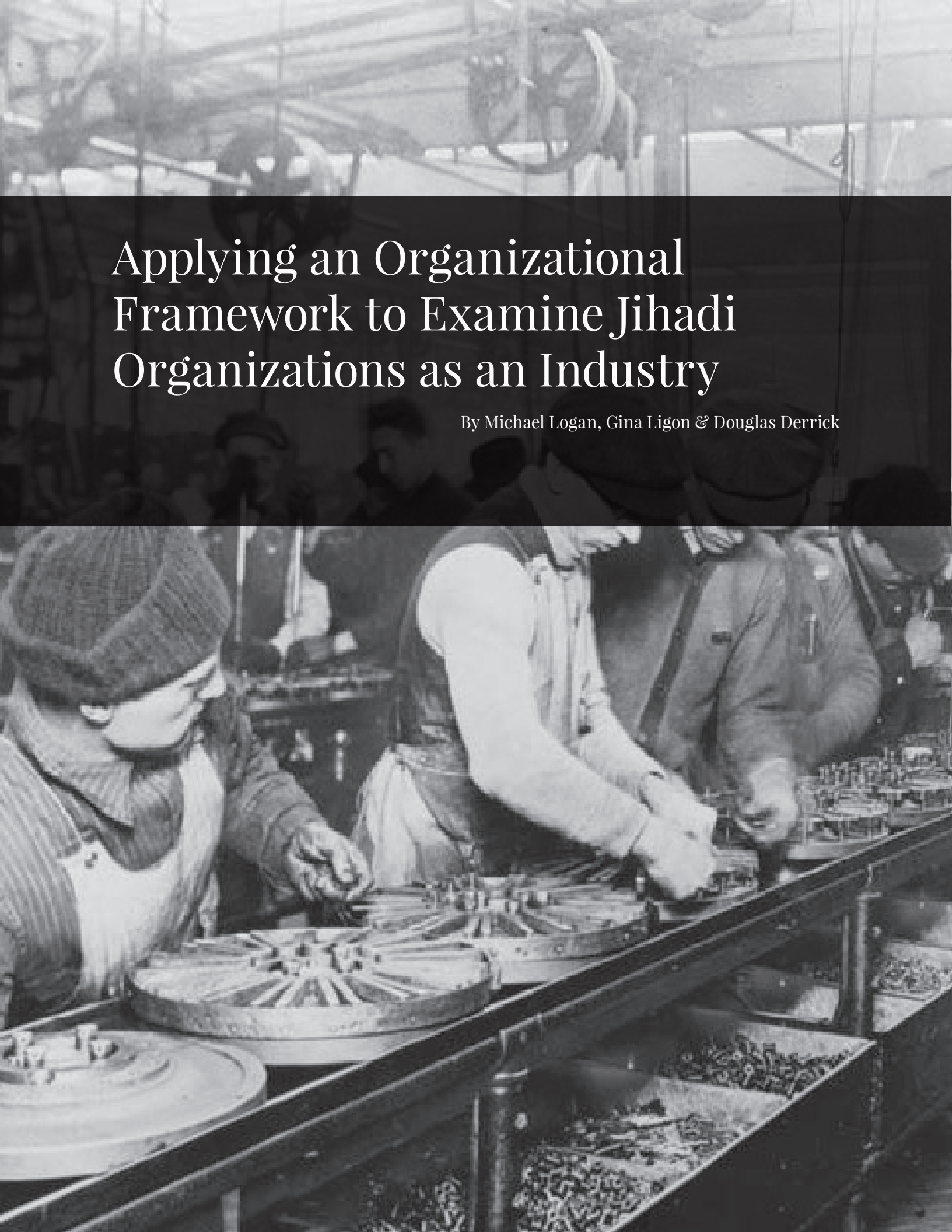
About the Author

Mr. Phillip Osborn, Supervisory Special Agent (ret.), is a 35 year law enforcement veteran who has spent well over 2 decades conducting and leading computer and Internet related investigations and operations. Mr. Osborn has served as the chairman of the World Customs Organization Electronic Crimes Experts Group, and he has represented the U.S. Government as a subject matter expert on cyber related topics to numerous national and international organizations. Some of his work dating from the early 1990s provided the foundation and motivation for the establishment of U.S. Customs Cyber Crimes Center, as well as the creation of the Internet Crimes Against Children Task Forces. For over 7 years he served as the U.S. Customs/ICE National Program Manager for Cyber Crimes, leading operations, investigations, and policy initiatives to address homeland and national security threats. One particular initiative he championed was in the area of the convergence of traditional border security with the cyber domain. Mr. Osborn earned his graduate degree in homeland security studies from the Naval Postgraduate School, and has completed other graduate work in information security and in global strategic intelligence studies. Mr. Osborn's most recent assignments prior to retirement were leading a DHS border security and tactical intelligence initiative, and serving as the director of a joint DHS cybercrime task force. He may be reached at iamoz@comcast.net.

Notes

- 1** National Oceanographic and Atmospheric Administration- Office of Coast Survey, https://www.nauticalcharts.noaa.gov/staff/law_of_sea.html (accessed March 2, 2017).
- 2** Ibid.
- 3** Stephen R. Viña, "Protecting Our Perimeter: 'Border Searches' Under the Fourth Amendment," (Congressional Research Service The Library of Congress, August 2006), 7.
- 4** Ibid,7.
- 5** Ibid, 6.
- 6** Ibid, 6.
- 7** Ibid, 8.
- 8** See 19 CFR 162.6 - Search of persons, baggage, and merchandise.
- 9** See 19 CFR 146.1 - Definitions
- 10** Ibid.
- 11** US Customs and Border Protection Policy Regarding Border Search of Information, https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf, (accessed March 2, 2017).
- 12** Ibid, 4.

Copyright © 2017 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



Applying an Organizational Framework to Examine Jihadi Organizations as an Industry

By Michael Logan, Gina Ligon & Douglas Derrick

Abstract

The Leadership of the Extreme and Dangerous for Innovative Results (LEADIR) project, funded by The Department of Homeland Security, Science and Technology Directorate, Office of University Programs (DHS S&T OUP) since 2010, uses an industrial and organizational psychology approach to assess the characteristics of violent extremist organizations (VEOs) in relation to their capacity for innovative and violent performance. In the current paper, we use the LEADIR database and an internal strategic organizational approach to assess the unique set of resources and capabilities that provide a competitive advantage within the “Jihad Industry.” The results suggest that VEOs ability to utilize or acquire one or more unique resources or capabilities provides a competitive advantage over other groups in the larger Jihadi Industry. We will discuss practical implications for DHS I&A, as well as the methodological contributions of using a lens from management theory and organizational psychology to the scholarship on violent extremism.

Suggested Citation

Logan, Michael, Gina Ligon, and Douglas Derrick. “Applying an Organizational Framework to Examine Jihadi Organizations as an Industry.” *Homeland Security Affairs* 13, Article 6 (October 2017). <https://www.hsaj.org/articles/14097>

Introduction

While the amount of research on violent extremism has increased since the terrorist attacks on September 11, 2001, only a handful of studies have delved into the complexities of violent extremist organizations.¹ Broadly speaking, violent extremist organizations (VEOs) are coordinated efforts among individuals that share a similar ideological framework and employ violence as a means toward a collective goal.² In terms of their sophistication, VEOs can range from relatively simple (e.g., Animal Liberation Front) to highly complex organizations (e.g., Da’esh). Regardless, VEOs are marked by a shared ideology as well as common organizational goals that are necessary for the group’s survival such as recruitment, fundraising, training, and disseminating information.

In the current paper, we use models from industrial and organizational (I/O) psychology and management to examine ten VEOs with a foothold in the “Jihadi Industry.” More specifically, we use the Leadership of the Extreme and Dangerous for Innovative Results (LEADIR) project to gain insight and differentiate VEOs relative to their peer organizations in terms of capability, resilience, and attractiveness. We performed a Value, Rareness, Imitability, Organization (VRIO) analysis³ to assess each VEO’s unique set of strategic resources (e.g., cyber infrastructure) and capabilities (e.g., tactical innovation) that provide a competitive advantage among their industry peers.

The results of our analysis offer general and operational-level implications. More specifically, at a general-level, this study highlights:

1. The robust nature of using an organizational approach to examine and differentiate VEOs. In particular, this approach may prove useful for agencies in identifying high versus low risk threats, and allocating resources to combat those threats.
2. A novel approach to gather, quantify, and compare the cyber capabilities of VEOs. While prior research on VEOs' use of cyber has focused solely on descriptions of use of publicly-available social media platforms (e.g., Twitter, YouTube) or encrypted forums, our contribution is that we systematically analyzed what cyber innovation means in the Jihadi Industry by assessing the underlying behaviors facilitated by their use of an array of platforms and web-based features.

Next, at the operational level our analysis suggests:

1. Da'esh leads the Jihadi Industry on all performance metrics, but they have been significantly degraded since 2014. Examining their cyber presence, our data shows less collaboration across domains and fewer durable cyber objects produced since the end of 2015. Thus, using organizational metrics such as collaboration in both physical and cyber space can provide CT professionals with a unique metric for the effectiveness of capturing digital terrain and degrading the organization.
2. Al Qaeda in the Arabian Peninsula (AQAP) and Jabhat Fatah al-Sham (JFS) (formerly al-Nusra Front) are only second to Da'esh in terms of organizational legitimacy efforts, leadership and human capital, and fundraising. Similar to Da'esh, AQAP's long-term tenure within a turbulent environment (e.g., Yemen) has created an efficient, legitimate, and sophisticated organization profile. Likewise, JFS has effectively played on the grievances of the Sunni populace by branding themselves as a viable group that is different from Al Qaeda Central. The method of examining organizational capacity can provide an early warning indicator of growing strength for emerging threats.
3. Despite over a decade of international pressure, Lashkar-e-Taiba (LeT) continues to operate with impunity in Pakistan. In turn, LeT is one of the most effective VEOs at fundraising in the Jihadi Industry. Fundraising as a sustained advantage for LeT is concerning and should be closely monitored given the establishment of al Qaeda's new affiliate in the Indian Subcontinent.
4. Abu Sayyaf Group (ASG) and, to a slightly lesser extent, Al Qaeda in the Islamic Maghreb (AQIM) performed poorly across most indices in our analysis. In-fighting between high-ranking members of each organization as well as successful counter-terrorism operations have diminished the capacity of each group. ASG and AQIM are the least likely to acquire the resources to sustain a competitive advantage compared to the other organizations in this analysis.

In the following section, we provide an overview of the methodology used for this study as well as a more in-depth discussion of our findings.

Methodology

This project employed a historiometric methodology in order to evaluate the strategic and comparative threat posed by VEOs within the Jihadi Industry. Following best practices⁴, we defined the sample that would provide the best comparative attributes to evaluate some of the most prominent VEOs within the larger framework of high threat VEOs. After identifying the sample, we gathered data from primary and secondary sources, evaluated the organizations in our sample using the LEADIR content coding scheme and indices of technical capabilities and sophistication.⁵ Finally, we conducted analyses to identify organizational attributes and resources that differentiate certain VEOs and their competition in the Jihadi Industry. Figure 1 provides a visual representation of the methods used for this study.

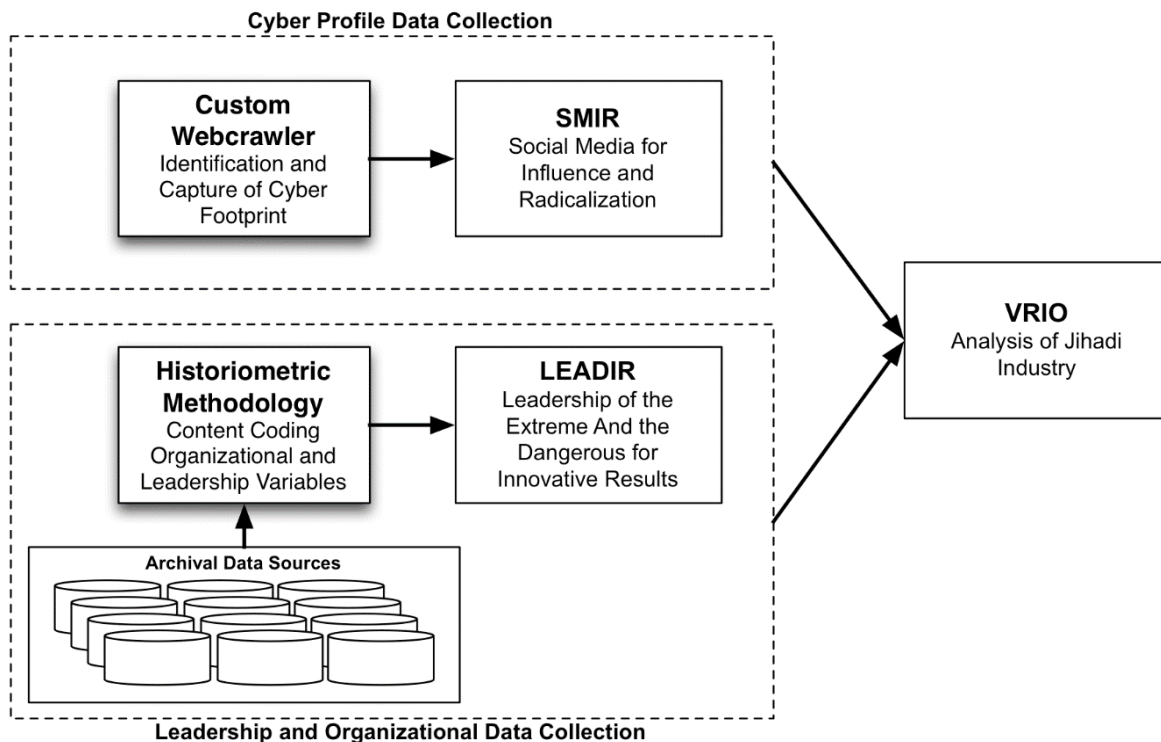


Figure 1. Overview of Methods

Data Collection and Procedure

We partnered with three government-civilian subject matter experts (SMEs) familiar with the Jihadi Industry to select key VEOs whose ideology is centered on Salafist conceptions of Jihad. Specifically, we focused on Da'esh and its affiliates as well as affiliates of al Qaeda Central (AQC). Given that Da'esh was formerly an affiliate of AQC, this was considered the most appropriate sample for comparison, because by virtue of forming those alliances (with the exception, perhaps, of AQAP), the ideology, tactical operations, and targeting preferences of the affiliates were shaped by AQC. Table 1 highlights the ten VEOs being examined.

Table 1. Sample of Ten VEOs

VEO	Primary Area(s) of Operation
1) Da'esh	Iraq, Syria
2) Jabhat Fateh al-Sham (JFS)	Iraq, Syria
3) al Qaeda in the Islamic Maghreb (AQIM)	Algeria, Mali
4) al Qaeda in the Arabian Peninsula (AQAP)	Yemen
5) al-Shabaab	Somalia
6) Boko Haram	Nigeria, Cameroon, Niger, Chad
7) Afghan Taliban	Afghanistan, Pakistan
8) Tehrik-e-Taliban (TTP)	Pakistan, Afghanistan
9) Lashkar-e-Taiba (LeT)	Pakistan
10) Abu Sayyaf Group (ASG)	Philippines, Indonesia

Organizational and Leadership Data

To gather information about these organizations, secondary data were gathered from academic and government sources (e.g., profiles and data from the National Consortium for the Study of Terrorism and Responses to Terrorism (START), Southern Poverty Law Center, Mapping Militant Organizations by Martha Crenshaw) as well as scholarly case studies and public-records databases (e.g., Lexis-Nexis). In some cases, we triangulated these secondary sources by using source-verified primary documents from the organizations themselves, such as manuals, propaganda, videos, and websites run by the organizations to cross-reference information found in archival, analyst reports (e.g., START resources).

Since one of our main research objectives for this paper was to identify key areas where VEOs in our sample differ, we used a psychometric approach to scale development and criterion from previous LEADIR projects⁶ to code and classify the organizational-level data. For each category of variables (i.e., organizational characteristics, performance-related constructs, and controls), operational definitions with readily identifiable benchmark examples were used, employing psychometric best practices used to evaluate other types of heterogeneous organizations

Attack and Cyber Data

The attack-level data in this study were drawn from the Global Terrorism Database (GTD). Rather than simply assessing lethality as an indicator of performance, we performed a stratified random sample of each VEO's attacks as reported by the GTD and applied an innovative coding scheme to each one⁷. In total, 27 rating scales were applied to 1,441 attacks across the ten VEOs in our sample.

To assess cyber sophistication and expertise, we collected and analyzed web material associated with each VEO. The data was collected through a combination of "key word" searches and the utilization of an automated web crawler. After collection, the cyber data were evaluated by technical SMEs to determine the sophistication of the resources and

expertise that would be required to produce them. For example, webpages that had multiple indices of encryption capabilities were evaluated as more sophisticated than those with fewer security parameters deployed.

Analytic Strategy: VRIO Analysis

To compare the ten Jihadi Industry VEOs, we used a VRIO analytic technique, or a technique that evaluates the likelihood that an organization will obtain a sustainable advantage based on its resources.⁸ Competitive advantage references an organization's ability to create more value than its rivals, and requires SMEs to assess each VEO's resources on 1) their value, b) rarity, c) inimitability, and d) the degree the other resources in an organization are organized effectively to take full advantage of that advantage. Organizations possessing only *valuable* resources and capabilities are expected to perform the same as all other organizations in the industry (i.e., competitive parity). Organizations possessing valuable and rare resources and capabilities are expected to perform *better* than other organizations but only for a short period of time (i.e., temporary competitive advantage), while organizations possessing *valuable, rare, and imperfectly imitable* resources and capabilities are expected to demonstrate a long-term advantage (i.e., sustained competitive advantage). Imperfect imitability of a resource or capability was determined by the presence of one or more of the following attributes.

1. History – The focal resource or capability was acquired at a *particular* place and time in the past. Competing organizations are unable to imitate that resource or capability because they are operating in a different place and time (e.g., senior military leadership of ISIL who came from Saddam Hussein's regime).
2. Causal ambiguity – Competing organizations are unable to imitate the focal resource or capability because of its complexity, tacit, and/or intangible attributes (e.g., social media and cyber sophistication).
3. Social complexity – Competing organizations are unable to replicate the focal resource or capability due to its presence within a sectarian conflict that has its own magnetism (e.g., public discontent with the Assad regime).

The overall organization (i.e., its structure) must also be aligned in such a way as to take advantage of the resources or capabilities in question. If misaligned, competitive disadvantages may emerge even though resources and capabilities are valuable, rare and difficult to imitate. VRIO analyses evaluate the likelihood that an organization will obtain a sustainable advantage in a given competitive arena. Sustainable competitive advantages are assumed to originate from the resources and capabilities controlled by the organization.

Strategically Differentiating Resources

Resources represent the tangible and intangible assets controlled by the organization. Resources can be financial (e.g., cash), physical (e.g., equipment, natural resources), human (e.g., knowledge, intelligence, training, creativity) and organizational (e.g., reporting structure, culture, planning and control mechanisms). For the present effort—building upon the findings from our 2014 report on the VRIO of Da'esh compared to its competitors—we

assessed each of the ten VEOs in our Jihad Industry sample on six resources: (1) Marketing and Branding, (2) Recruiting and Human Capital, (3) Fundraising, (4) Tactical Innovation, (5) Cyber Sophistication, and (6) Cyber Interactivity. The subsequent sections provide more justification and detail into each VEO’s differentiators. Figure 2 shows the overall findings from our VRIO analysis. In the following sections, we describe the subsections of the VRIO analysis in more detail as well as provide illustrative examples of high-and-low performance.

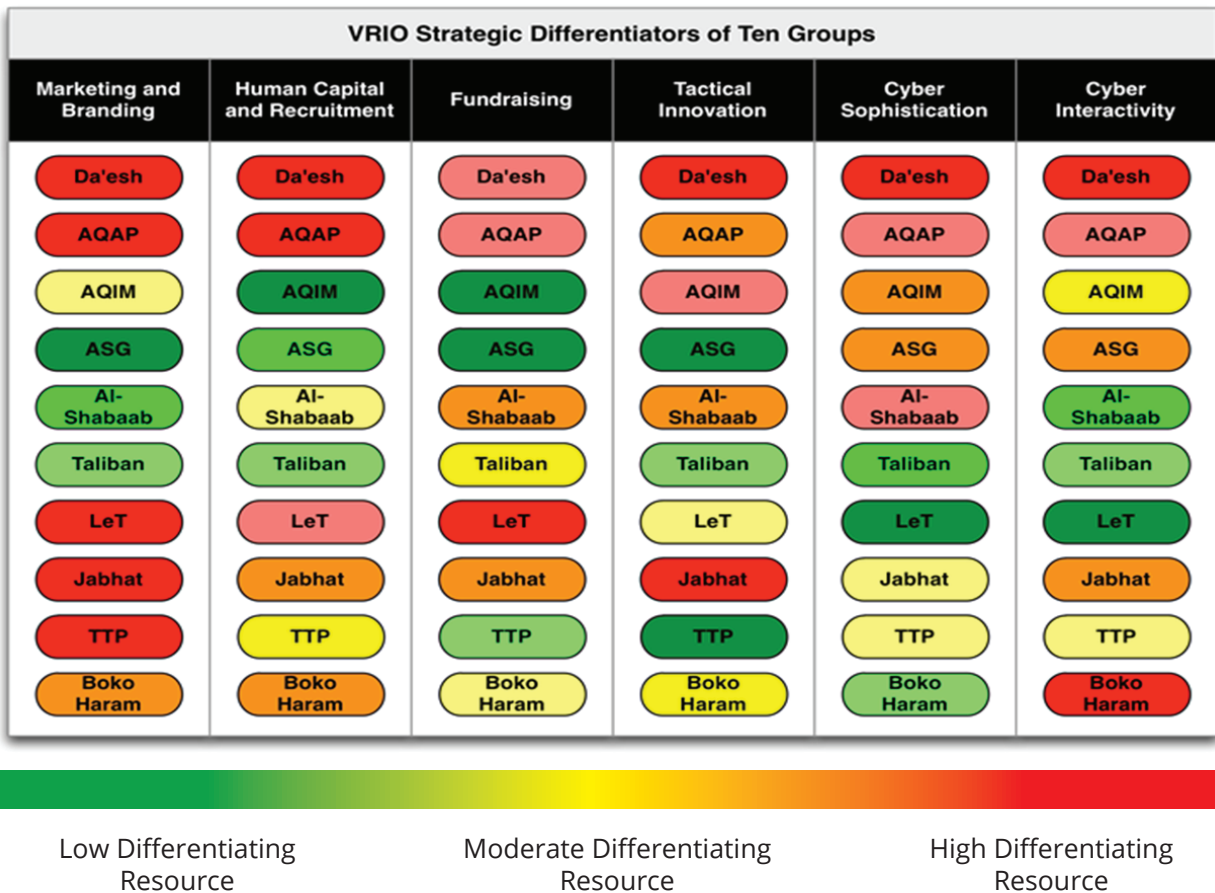


Figure 2. VRIO of Ten VEOs

Marketing and Branding

An organization’s brand can be described as its personality. Like individuals and other firms, each VEO has a unique personality that is shaped by the VEO itself and the consumers of its products. A branding and marketing strategy can be understood as complementary components to an organization’s outreach. The brand is the representation and staple of the organization, while marketing is comprised of the behaviors the organization undertakes to sell its brand. In other words, marketing behavior is how an organization sells its brand or its personality. VEOs, like other organizations, put forth effort to establish themselves as a unique brand within the terrorism field and therefore engage in similar strategies like traditional firms, such as the production of media favoring the brand.

For this analysis, we used two measures of reputation and prominence to gauge the effectiveness of the marketing and branding of the ten VEOs. An organization's brand is largely built in the relative reputation or status that organization has. This status can be understood as how popular or well-known a certain organization is within its industry. In our analysis, this industry would be the "Jihad Industry." Therefore, we used cultural and comparative reputation to measure the degree to which each VEO compares in status against other organizations within the industry. Prominence is a multiplicative index measuring both the level of co-branding and external legitimacy of an organization. The degree to which an organization allies or "co-brands" with another brand increases the performance and prominence of the organization and influences the relative understanding of the brand. For example, co-branding allows for two organizations to make use of the brand of the allied organization to further increase the prominence of its own brand and add to the relative performance of the other brand. This co-branding often leads to an increase in customers and resources because both brands can make use of the resources of the other brands. Meanwhile legitimacy is a measure of the degree to which an organization follows the rules of industry and is an indication of how the group is regarded as a "professional" within its field.

Table 2. Comparative VRIO rating

Performance on VRIO Analysis	VEO	Illustrative Example
High	AQAP	AQAP's <i>Inspire magazine</i> is one of the flagship English-language jihadi publications and is one of many propaganda magazines AQAP publishes. These publications are not only used to recruit, but also shape potential sympathizers and supporter's attitudes and perceptions of the group.
Low	Abu Sayyaf Group	In 2014, one of Abu Sayyaf Group's core leaders pledged allegiance to Da'esh. Despite this oath of allegiance, no credible link between the two groups has been found. Given the decline of Jemaah Islamiyah and their weakened relationship with al Qaeda Central, ASG lacks a clear linkage to the most prominent organizations in the current Jihadi Industry.

Human Capital and Recruitment

Like most organizations faced with increasing competition and growing external pressures, VEOs have realized that they too must evolve to meet emerging challenges. The current iteration of violent extremist organizations (VEOs) such as Da'esh, Al-Shabaab, and AQAP have been particularly successful at perpetrating violence and spreading fear through innovative means such as the utilization of social media and web-based platforms. The sampled VEOs are adept at building their ranks through a combination of both time-tested and increasingly novel personnel attraction and selection mechanisms. The importance

of knowledge about social, personal and economic factors for recruitment, as discussed above, is reinforced by research both on the nature of VEO propaganda. Zelin⁹ analyzed Da'esh social media output and identified that alongside promoting their military-related activities, the group highlighted their social services as well as “the great life one can live under the Caliphate, especially by foreign fighters.” Other VEO media seek to show their familiarity with western culture to attract western members; for example, posting pictures of fighters with Nutella jars.¹⁰ Da'esh spends significant energy presenting the view that they are active and on the march. Moreover, when communicating to potential recruits from the West, Da'esh has images that showcase both their military prowess and highlight their organizational legitimacy as well as couch pragmatic advice about travel and operations in ideological imperatives. This mix of pragmatic advice, ideology, and organizational legitimacy creates a powerful brand to influence potential recruits.¹¹ In LEADIR, we assess the techniques VEOs use to increase their human capital. Following from how recruitment is assessed in conventional organizations, we rate each VEO's tactics in terms of their novelty (degree of surprise or uniqueness in a given region and time), diversity (number of different types of techniques), and overall effectiveness (degree to which the recruiting strategies yield a viable pool of skilled members).

Table 3: Comparative VRIO rating¹²

Performance on VRIO Analysis	VEO	Illustrative Example
High	Da'esh	Until recently, Da'esh has been able to recruit an array of specialized recruits to the caliphate. Da'esh success in recruitment is largely due to their novel use of social media and other peer-to-peer cyber technologies.
Low	AQIM	AQIM primary targets low-skilled recruits through their regionally-focused, anti-colonialism propaganda. Despite operating their own media-wing, Al-Andalus Media, AQIM is said to lack the sophistication to recruit globally, outside of the Sahara and Sahel region of Northern Africa.

Fundraising

While it is difficult to assess the true wealth of any clandestine organization, LEADIR does have data to speak to the novelty of fundraising mechanisms used by a given VEO. Our benchmark scales require raters to compare VEOs based on low novelty fundraising tactics (e.g., membership dues) versus high novelty fundraising tactics (e.g., looting artifacts from the ancient city of Palmyra and selling them). For the present effort, we compared each VEO in our sample longitudinally to assess changes in the creativity of tactics to secure resources. Before turning to these results, however, we would like to point out two additional findings concerning fundraising. First, the relationship between novelty in fundraising and an organization's age tended to be inverse, which is to say that the longer the organization has been together, the less innovative their approach. The relationship is not linear, however, and organizations that have been together for approximately fifteen years are more innovative than those who have been together for ten years, but are less innovative

than those which are relatively new (less than ten years). Second, the relationship between destructive fundraising tactics per monetary unit and an organization's age approximates a U-curve, indicating that the newest groups tend to have moderately destructive fundraising techniques. The oldest groups largely employed non-destructive fundraising tactics, while those that have been together for roughly fifteen years employed the most destructive fundraising tactics.

Table 4: Comparative VRIO rating

Performance on VRIO Analysis	VEO	Illustrative Example
High	LeT	LeT relies very little on coercive or illegal methods to secure funds. Instead, LeT has established a stable infrastructure through an expansive network of private and public donors and charitable organizations.
Low	TTP	TTP relies heavily on illegal activities to secure funds (e.g., drug trade, kidnapping, bank robberies). These funding streams may provide short-term success, but do not provide a long-term, sustainable funding solution.

Tactical Innovation

Organizations within the Jihadi Industry operate in a turbulent environment with immense competition over human capital, which is drawn to a Salafist Jihad ideology. In order to survive, VEOs must work toward creative goals and, more importantly, develop innovative ways to thrive in an unpredictable market. Tactical innovation or the extent to which VEOs "adopt news methods or means of violence"¹³ provides one indicator of creativity and innovation. To illustrate VEOs capacity for tactical innovation, we conducted an exploratory factor analysis on the attack-level variables in our sample. A total of 1,441 attacks were coded yearly for each VEO in our sample and variables were explored using a principal component analysis (PCA) with varimax rotation. The PCA resulted in eight items loading on two different constructs. The first factor included three items pertaining to markers of originality and expertise. This factor was named *Unique Proficiency* and describes attacks that require expertise and are unique in terms of the weapons used and methods employed. The second factor included five items pertaining to complexity and physical infrastructural damage. This factor was named *Attack Sophistication* and is characterized by highly coordinated, well-executed

attacks that often cause major infrastructural damage. The two factors were moderately correlated ($r = .359$, $p < .01$).

Table 5. Average Tactical Innovation Scores (n=1,441)

VEO	Unique Proficiency	Attack Sophistication
Afghani Taliban	5.87	9.39
Jabhat Fatah al-Sham	8.53	11.00
Al-Shabaab	7.34	9.86
AQAP	6.29	11.28
AQIM	6.91	11.81
Abu Sayaaf Group	5.17	7.75
Boko Haram	5.53	11.33
Da'esh	7.29	12.13
LeT	6.25	11.00
TTP	5.08	8.27
1) Unique Proficiency ranges from 3-13; Attack Sophistication ranges from 5-20.		
2) Higher scores on both constructs indicate stronger performance.		

Each VEO's average *Unique Proficiency* and *Attack Sophistication* scores were used to guide the VRIO analysis and act as a descriptive indicator of each organization's capacity for tactical innovation. Above, Table 2 shows that there was relative consistency in each organization score across both measures. For example, Da'esh, Jabhat Fateh al-Sham, AQIM, and AQAP scored in the upper half on both *Unique Proficiency* and *Attack Sophistication*, while the Afghan Taliban, LeT, TTP, and Abu Sayyaf Group scored in the bottom half. Two groups, Al-Shabaab and Boko Haram, were less consistent, scoring highly on one construct, but not the other. Al-Shabaab rated second only to Jabhat Fateh al-Sham in *Unique Proficiency*, yet scored in the bottom half on *Attack Sophistication*. Boko Haram had the third highest average *Attack Sophistication* rating, but scored poorly on *Unique Proficiency*.

Cyber Sophistication and Interactivity

Because the examination of cyber profiles of VEOs is relatively new, we first provide an overview of how the VEOs in our sample use cyber resources to execute organizational functions such as marketing, recruiting, fundraising, and attack planning. VEOs leverage domains with low barriers and low authentication in order to host the content in the open as long as possible. There are several different patterns considering page and content posting and attributes. Page attributes fall under one of three distinct aspects; those who view pages for the group membership or loyalty; up- and down- loading of content; or content

engagement. This is confirmed by the results of an exploratory factor analysis of the web content we harvested with varimax rotation. Nine items obtained loading scores of .80 or higher across two different constructs. The four items loading on the first factor pertained to markers of complexity and the variety of features employed. This factor was named *Sophistication* and designates increasing technological skills and instantiations employed in message and content delivery by VEOs online. The five items loading on the second factor largely pertained to the facilitation of (social) ties between actors in the network. This factor was named *Social Interactivity* and is interactivity between actors in the social graph, including two types of direct message exchanges. The two factors were moderately correlated ($r = .46$, $p < .01$).¹⁴

Table 6. Cyber Sophistication and Social Interactivity Scores

VEO	Sophistication	Social Interactivity
Afghani Taliban	.30	.32
Jabhat Fatah al-Sham	3.11	2.16
Al-Shabaab	5.24	.27
AQAP	7.76	2.58
AQIM	3.81	.66
Abu Sayaaf Group	3.43	2.20
Boko Haram	1.71	3.20
Da'esh	10.05	5.34
LeT	---	---
TTP	2.05	.55

1) Higher scores on both constructs indicate stronger performance.
2) No transient webpages were found for LeT.

To assess each VEO on these factors, we obtained scores on each factor across their cyber objects. Table 3 indicates that while Da'esh is the most sophisticated and holds the most capability for social interactivity, AQAP is a close second on all metrics. In addition, while Boko Haram scored high on social media interactivity, it appears that they leverage existing open architecture in predictable ways. Thus, they may not have the cyber capability to program or innovate similarly to Da'esh, AQAP, or al-Shabaab. Interestingly LeT and Taliban have the lowest cyber capabilities. The main contribution from this analysis is that our process for assessing differences in the innovation and social media interactivity of these 10 VEOs allowed us to array the Jihadi Industry VEOs in the present sample. This has implications for their capacity to recruit and share their messaging, raise funds, and execute command and control.

Conclusions and Implications

The paper's main findings indicate that leadership, organizational structure, and innovation vary across the Jihadi Industry, which has implications for how government resources should be allocated for monitoring and analysis. In addition, the findings highlight the need for additional research to determine advanced indicator and warning signals of which groups will emerge as the most strategically differentiated and capable of malevolent innovation in coming years.

First, Da'esh leads the Jihadi Industry on all performance metrics, but they have been significantly degraded since 2014. Across leadership, organizational structure, marketing, attacks, and cyber capabilities, Da'esh outperformed each VEO in the present sample of the Jihadi Industry. However, since our last assessment of their human capital in 2014, the quality of leader talent and innovation of attack sophistication have diminished.

Second, we developed a method to gather, quantify, and compare VEO cyber sophistication and social media interactivity, and this custom method statistically differentiated the ten VEOs in our sample. Most of the research to date on VEOs' use of cyber has focused solely on descriptions of use of publicly-available social media platforms (e.g., Twitter, YouTube) or encrypted forums. Our contribution is that we systematically analyzed what cyber innovation means in the Jihadi Industry by assessing the underlying behaviors facilitated by their use of an array of platforms and web-based features.

Finally, conflict between top management team members are related to lower organizational capabilities and less innovation. The clearest example of this in our dataset is that of the Afghan Taliban, who should be poised for high levels of performance given their strategic location, third party endorsement by al-Qaida Central leaders, and organizational age. Despite these resources, infighting among leaders and lack of clear leadership mission has resulted in a less capable organization. Conversely, organizations such as Jabhat Fateh al-Sham and Da'esh gain strength under the stewardship of a mix of pragmatic and ideological leaders working collaboratively toward organizational goals.

These findings lead to the recommendations flowing from the present effort. First, monitor AQAP's rebrand efforts in Yemen, as well as outreach to Foreign Terrorist Fighters abroad. Al-Qa'ida in the Arabian Peninsula (AQAP) has been the most capable AQ branch, and its marketing efforts indicate a pivot to focus on the social services it provides as well as the resilience of its organizational structure despite leader losses. Given the nexus of the state-sponsored groups, failed/ fragile state markers, and crime-laden territory of Yemen, this group is poised for a re-emergence by all indicators. In addition, the high degree of social interactivity on various AQAP cyber platforms raises warnings for their potential outreach to those capable of executing a large-scale, sophisticated attack outside their territory.

Finally, focus strategic communication efforts and operational planning to denigrate VEO leadership. Success from efforts to degrade the Da'esh organization should highlight at least one practice to continue and increase: leadership targeting. While leadership targeting has mixed results, VEOs in our sample with the strongest cadre of leaders and a collaborative leadership team also have the most sophisticated attacks, cyber presence, and fundraising portfolio. Rather than focusing on the capacity of any one individual in a leadership position, it's critical that policy makers focus strategic communications and planning on disrupting the organizational dynamics afforded by an adversary's diverse and collaborative leadership team.

About the Authors

Michael Logan is a third-year doctoral student in the School of Criminology and Criminal Justice at the University of Nebraska Omaha. He holds a master's degree in criminal justice from Radford University and a bachelor's degree in criminology from Lynchburg College. His research interests focus on the organizational structure and leadership of violent extremist organizations (VEOs), individual-level risk factors for participation in violent extremism, and far-left extremism more broadly. Michael has worked on projects funded by the Department of Homeland Security (DHS) and the National Consortium of Studies of Terrorism and Responses to Terrorism (START). Michael is currently working alongside Dr. Gina Ligon on the Leadership of the Extreme and Dangerous for Innovation Results (L.E.A.D.I.R.) database and research that explores markers of malevolent creativity and innovation among VEOs. He may be reached at mlogan@unomaha.edu.

Gina Ligon is an Associate Professor of Management and Collaboration Science at the University of Nebraska at Omaha. She received her PhD in Industrial and Organizational Psychology with a Minor in Measurement and Statistics from the University of Oklahoma. She is a Principal Investigator at the National Consortium of Studies of Terrorism and Responses to Terrorism (START), examining the leadership and performance of transnational Violent Extremist Organizations (VEOs). Her research interests include profiling leaders from afar, violent ideological groups, expertise and leadership development, and collaboration management. She has published in the areas of leadership, innovation, and violent groups, and she is the Editor of the academic journal *Dynamics of Asymmetric Conflict: Pathways toward Genocide and Terrorism*. She may be reached at gligon@unomaha.edu.

Douglas C. Derrick is an Associate Professor of IT Innovation at the University of Nebraska Omaha and received his PhD in Management Information Systems from the University of Arizona. He holds a Master's degree in Computer Science from Texas A&M University and a Master's degree in Business of Administration from San Jose State University. He is a Distinguished Graduate (top 6%) from the United States Air Force Academy. His research interests include innovation, human-agent interactions, intelligent agents, decision support systems, and persuasive technology. Prior to joining UNO, Dr. Derrick worked as a Program Manager at MacAulay-Brown, Inc. and also served as an Air Force Officer. He has extensive experience as a DoD contractor, and he has been awarded contracts and grants from the Department of Defense, the National Science Foundation, and the Department of Homeland Security. Doug has published in journals and conferences including: *Journal of Management Information Systems*, *IEEE Intelligent Systems*, *AIS Transactions on Human-Computer Interactions*, *Group Decision and Negotiation*, Hawaii International Conference on System Sciences, IEEE International Conference on Intelligence and Security Informatics and IEEE International Carnahan Conference on Security Technology. He may be reached at dcderrick@unomaha.edu.

Notes


- 1 V. Asal, and R.K. Rethemeyer, "The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks," *The Journal of Politics*, 70, no.2, (2008):437-449; A.N.Celso, "Al Qaeda's Post-9/11 Organizational Structure and Strategy: The Role of Islamist Regional Affiliates," *Mediterranean Quarterly* 23, no.2, (2012):30-41; M.Crenshaw, "The Causes of Terrorism," *Comparative Politics*, 13, no.4, (1981):379-399; J.Jung and J.Lee, "Organizational Behavior of Terrorist Groups," *Journal of Public Administration and Governance*, 5, no.2, (2015): 62-77; G.S. Ligon, M. Harms, and D.C Derrick, "Lethal Brands: How VEOs Build Reputations," *Journal of Strategic Security* 8 no.1, 27; B.Mendelsohn, *The al-Qaeda Franchise: The Expansion of al-Qaeda and Its Consequences*, (New York: Oxford University Press, 2016); J.N. Shapiro, *The Terrorist's Dilemma: Managing Violent Covert Organizations*, (Princeton, NJ: Princeton University Press, 2013).
- 2 See Ligon, et al., "Putting the "O" in VEOs: What Makes An Organization?" *Dynamics of Asymmetric Conflict*, 6, no.1,(2013): 110-134.
- 3 A VRIO analysis is an acronym for a four-question framework used to determine the competitive potential of a resource or capability in terms of whether it is valuable, rare, easy/difficult to imitate, and susceptible to exploitation by the organization. G.Ligon, S.Hunter, and D.Harris, "Quantifying Leader Lives: What Historiometric Approaches Can Tell Us," *The Leadership Quarterly* 23, 1104-1133.
- 4 Ibid.
- 5 G. Ligon, M. Harms, and D.Harris, *Leadership of the Extreme and Dangerous for Innovative Results*, Project completed for the START consortium.
- 6 G.Ligon, et al., *Organizational Determinants of Violence and Performance: Introducing the START L.E.A.D.I.R. (2013) Study and Dataset*. Project completed for the START consortium; G.Ligon, M.Harms, and D.Harris, *Leadership of the Extreme and Dangerous for Innovative Results*. (2014) Project completed for the START consortium; G. Ligon, et al., *The Jihadi Industry: Assessing the Organizational, Leadership, and Cyber Profiles*, (2017) Project completed for the START consortium.
- 7 We assessed each attack for elements of sophistication such as 1) degree of coordination required, 2) amount of technical expertise needed, 3) symbolic nature of the target, and 4) amount of destruction to people, processes, property, and/or symbols of the target.
- 8 J. Barney, "Firm Resources and Sustained Competitive Advantage," *Journal of Management*, 17, 99-120.
- 9 A.Y. Zelin, "Picture or It Didn't Happen: A Snapshot of the Islamic State's Official Media Output," *Perspectives on Terrorism* 9 no.4, Advance online publication retrieved from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/445/html>. ISSN 2334-3745.
- 10 S. Gates and S. Podder, "Social Media, Recruitment, Allegiance and the Islamic State," *Perspectives on Terrorism* 9 no.4, Advance online publication retrieved from <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/446/html>. ISSN 2334-3745.
- 11 D.C. Derrick et. al., "Ideological Rationality: A Cyber Profile of ISIL," *Dynamics of Asymmetric Conflict Journal* 9, no.1 (2016): 57-81.
- 12 C.S. Chivvis and A. Liepman, "North Africa's Menace: AQIM's Evolution and the U.S. Policy Response," RAND Corporation.
- 13 P. Gill et al., "Malevolent Creativity in Terrorist Organizations, ". *The Journal of Creative Behavior*, 47 no.2, (2013):125-151.
- 14 The factor analysis and bivariate correlation results for the "cyber sophistication and interactivity" section are available upon request from the first author.

Copyright © 2017 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs

By Duane Verner, Frederic Petit, and Kibaek Kim



Abstract

Protecting critical infrastructure, especially in a complex urban area or region, should focus on identifying and prioritizing potential failure points that would have the most severe consequences. Such prioritization can inform targeted planning and investment decisions, such as what infrastructure should be hardened or relocated first or what infrastructure should receive priority restoration following a disaster, among other uses. Without a prioritization process, assessment and protection programs are typically guided by intuition or expert judgement, and they often do not consider system-level resilience. While understanding how to prioritize high-consequence failure points for assessments and, for protection is essential, the complexity of infrastructure systems can quickly overwhelm. For example, in a notional region with 1,000 electric power assets, almost one million failure scenarios are associated with an N-2 contingency and nearly one billion failure scenarios are associated with an N-3 contingency. As a result, it is simply not feasible technically nor financially for system operators and government agencies to assess and prepare for all possible disruptions. Therefore, a primary goal of critical infrastructure protection and resilience programs should be to identify and prioritize the most critical contingencies affecting infrastructure systems. Achieving this goal will allow decision makers to identify high-impact isolated failures as well as cascading events, and to prioritize protection investments and restoration planning accordingly. To solve this problem, Argonne National Laboratory developed an optimization framework capable of modeling and prioritizing high-consequence failure points across critical infrastructure systems. The optimization framework can model at the system level or the interdependent “system-of-systems” level and is applicable to any infrastructure.

Suggested Citation

Verner, Duane, Frederic Petit, and Kibaek Kim. “Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs.” *Homeland Security Affairs* 13, Article 7 (October 2017). <https://www.hsaj.org/articles/14091>

Introduction

Argonne National Laboratory (Argonne) has developed an optimization algorithm and modeling framework capable of identifying the highest-consequence failure points within critical infrastructure systems. The optimization algorithm and framework can be applied to any infrastructure at the system level or the interdependent “system-of-systems” level and can be used to model any combination of infrastructure failures. Results from the optimization modeling can be used by analysts to identify priority assets for assessments and to assist infrastructure system owners and operators and government agencies when they are making critical infrastructure protection and mitigation investment decisions.

Understanding Infrastructure Failures

A fundamental component of critical infrastructure security and resilience programs should include understanding how, why, and where systems fail. This understanding should guide decisions on where to conduct in-depth assessments as well as which protection and mitigation measures to pursue. However, a complicating factor is that infrastructure failures vary significantly. Some failures will generate significant consequences at the system or regional level, whereas effects from other failures remain local, while still others have little to no effect on the overall service provided. For illustration purposes, Figure 1 shows a 345-kV electric power transmission system between a generator substation and a remote substation.

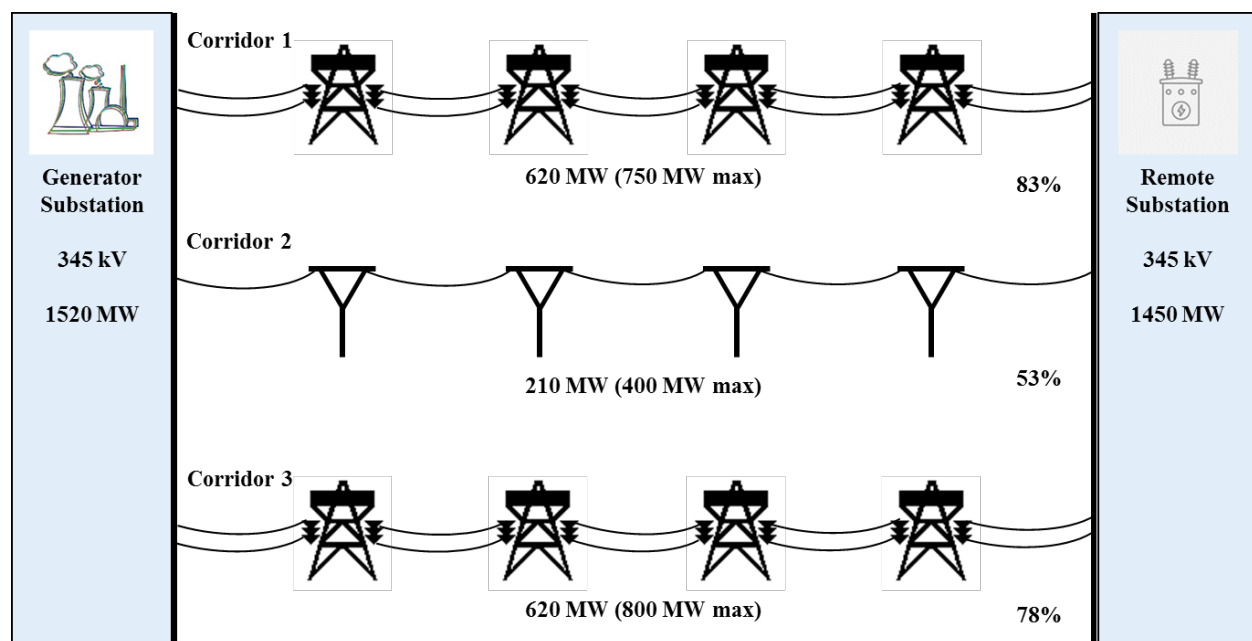


Figure 01. Electric Transmission Lines¹

In this example, the generation plant produces 1,520 MW² of power that is transported to the remote substation via three transmission corridors. Corridor 1 combines two circuits (lines) that allow transport of a maximum of 750 MW. Corridor 2 is a single circuit that allows transport of a maximum of 400 MW. Corridor 3 combines two circuits that allow transport of a maximum of 800 MW. By design, the three corridors operate below their maximum capacity levels, which allows for the relocation of power among the remaining circuits in the event of a disruption in one of them. For example, if the Corridor 2 circuit fails, the system's overall vulnerability will increase but it will not experience cascading system failure because the two other corridors can compensate for the loss (Figure 2).

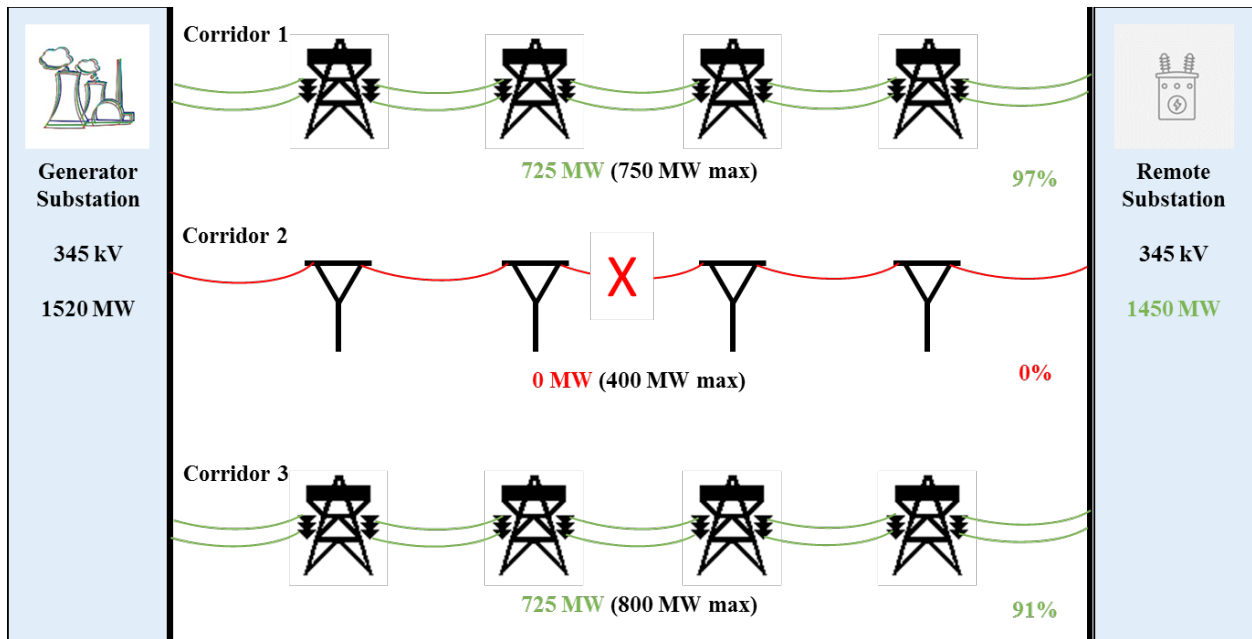


Figure 02. Loss of Corridor 2 Circuit

Corridor 1 circuits would operate at 97% of their capability and Corridor 3 circuits would operate at 91% of their capability. Similarly, the loss of one circuit from Corridor 1 would not trigger a cascading system failure because of the ability of the remaining circuits to compensate (Figure 3).

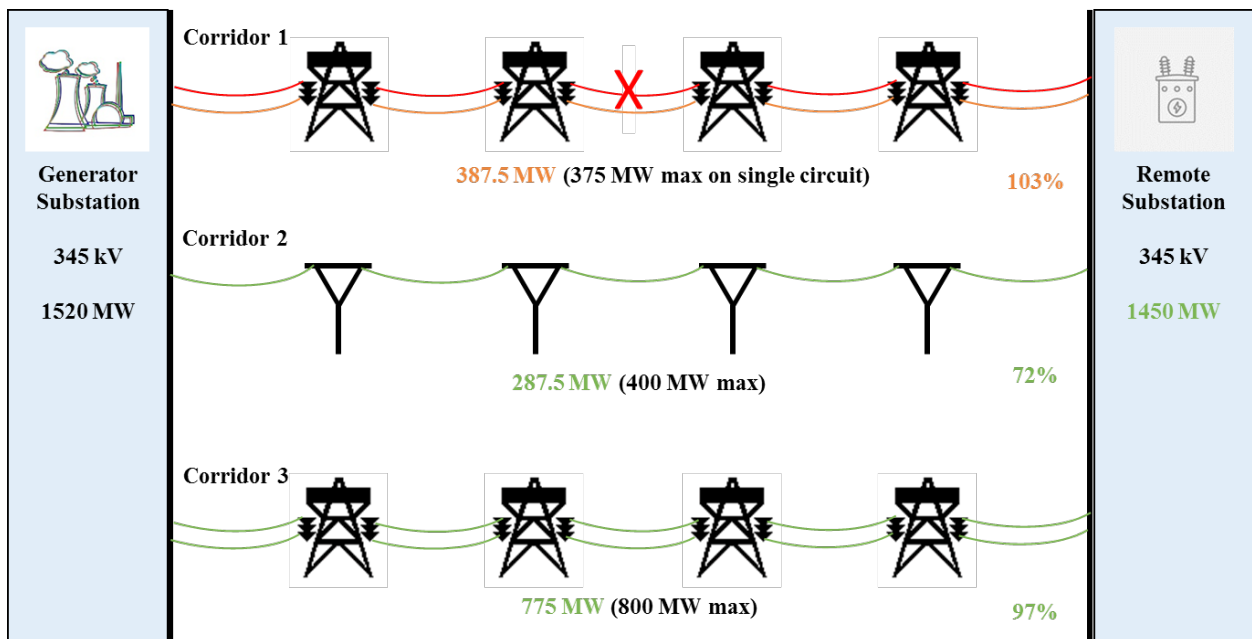


Figure 03. Loss of One Circuit in Corridor 1³

Building on the operating conditions identified in Figure 3, Corridor 3 would operate near full capacity (97%); Corridor 2 would operate at 72%; and the remaining circuit of Corridor 1 would operate at 103%, which, over time, could lead to the loss of the second circuit and therefore a failure of Corridor 1 (Figure 4).

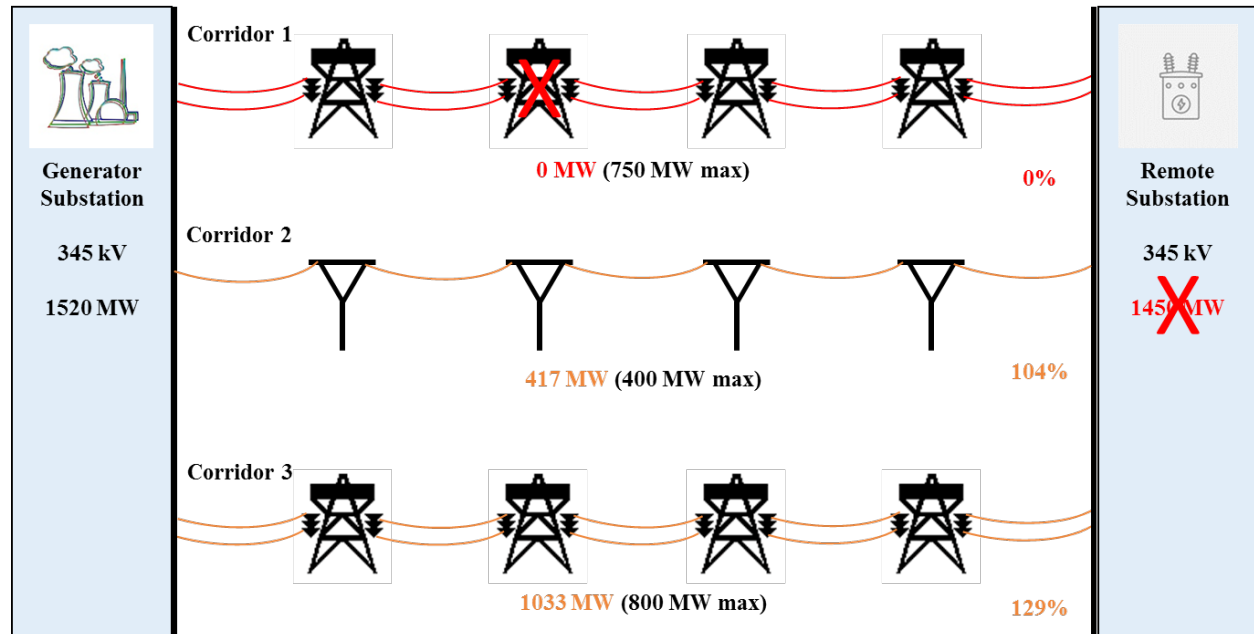


Figure 04. Loss of Two Circuits in Corridor 1

A loss of Corridor 1 would impede the ability of the two other corridors to operate safely. Corridor 2's circuit would operate at 104% of its capability, and Corridor 3's circuits would operate at 129% of their capability. Under this scenario, the circuits could begin to heat and ultimately trip, triggering a system failure. Assuming all other risk factors are equal, this simplified example shows that the consequence of disruption of Corridor 1 is greater than disruption of Corridor 2, and, as such, Corridor 1 should receive priority when making security and risk management decisions.

Infrastructure fails in many different ways with varying consequences. This N-1 contingency test shows that this system can sustain the disruption of Corridor 2. However, in our example, the loss of one circuit in Corridor 1 would generate an overuse of the remaining circuit in the corridor and could lead to additional consequences. The N-1 contingency can be mitigated by shedding some of the load to bring the transfer capability in Corridor 1 back to 100%, which could avoid problems leading to the N-2 contingency case. The N-2 contingency test, resulting in the total loss of the two circuits in Corridor 1, would cascade to the two other corridors and lead to an overall system failure.

While this section focused on electric power, there are many similar nuances associated with failures in other infrastructure. For example, within the telecommunications sector, loss of a cellular tower does not necessarily mean that your phone will lose service, the closing of a road does not always mean that you can't get to your destination, and so on. In other words, infrastructure system failures are not all created equal.

The Need for Prioritization

Without a prioritization process, infrastructure assessment, protection and mitigation programs are typically guided by intuition or expert judgement, and they often do not consider system-level reliability, redundancy, and overall resilience. While understanding how to prioritize high-consequence failure points for assessments and, for protection is essential, the complexity of infrastructure systems can quickly overwhelm decision-makers. For example, in a region with 1,000 electric power assets, almost one million failure scenarios are associated with an N-2 contingency, and nearly one billion failure scenarios are associated with an N-3 contingency (Figure 5). As a result, system operators and government agencies find it technically and financially prohibitive to assess and prepare for all possible disruptions.

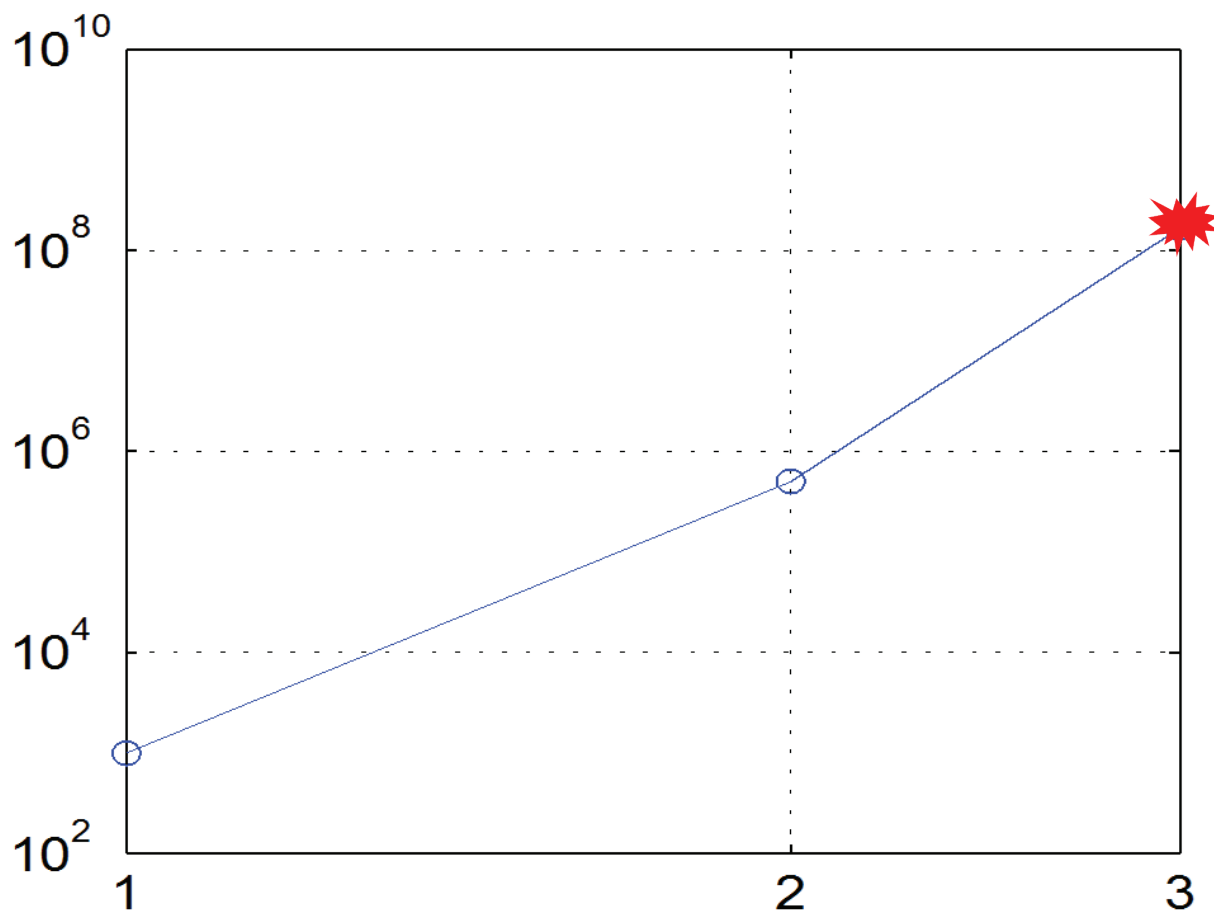


Figure 05. Possible Failure Scenarios with an N-3 Contingency for 1,000 Electric Power Assets

Therefore, a primary goal of critical infrastructure protection and resilience programs should be to identify and prioritize critical contingencies affecting infrastructure systems. Achieving this goal will allow decision makers to identify high-impact isolated infrastructure failures, as well as cascading events, and to prioritize protection investments and resilience planning accordingly. Such an approach should also consider infrastructure interdependencies.

Considering Infrastructure Interdependencies

Interdependencies among critical infrastructure assets increase risk to individual assets and the overall system. These interconnected infrastructure components constitute a “system of systems” where the failure of one or multiple infrastructure elements can cascade and affect the resilience of the entire system and ultimately the region. Figure 6 illustrates interdependencies among seven different infrastructure sectors and subsectors.

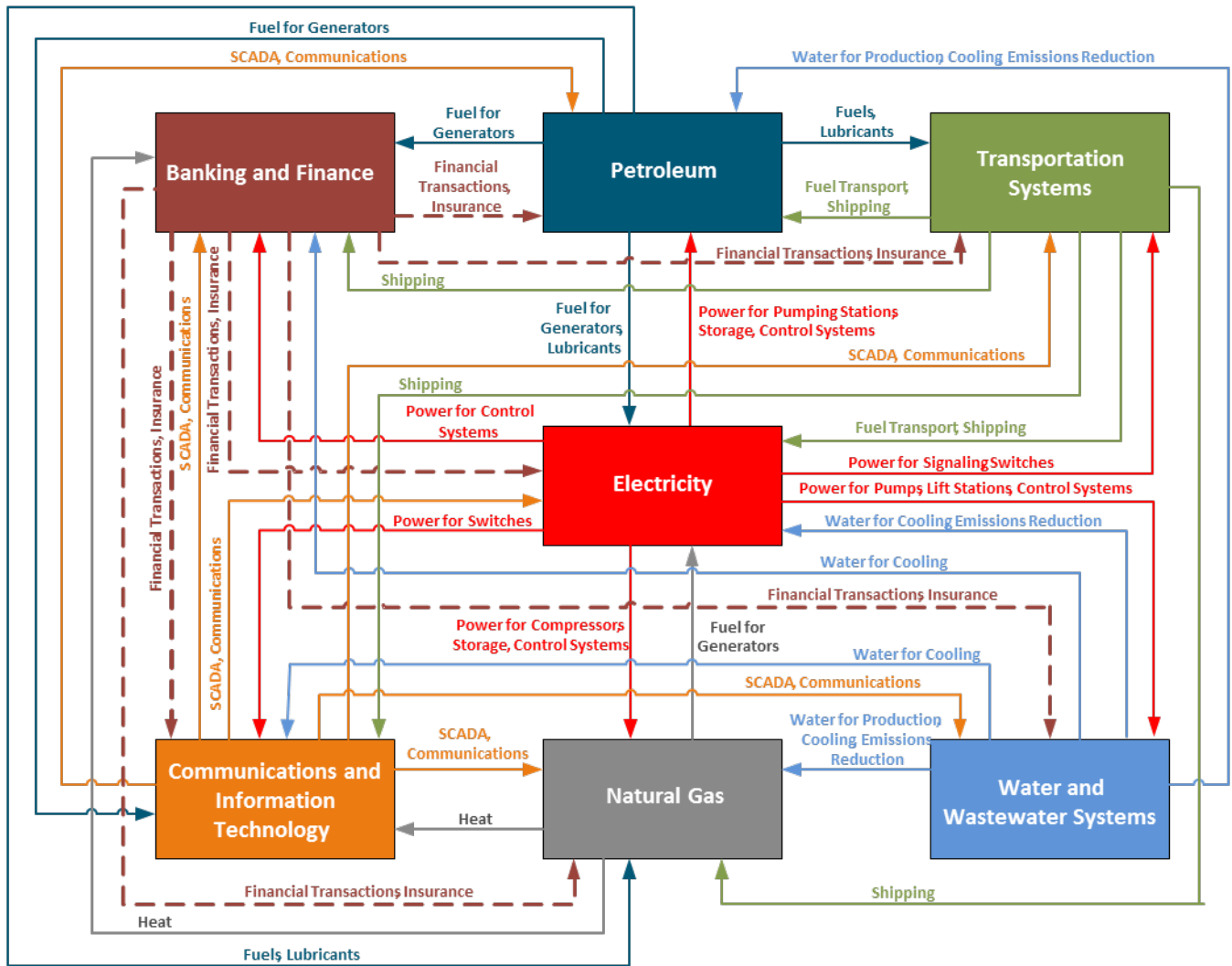


Figure 06. Critical Infrastructure Interdependencies⁴

However, as highlighted in the earlier electricity example, simply identifying connections between infrastructure does not provide a sufficient understanding of why or whether a connection is critical to the operational integrity of the system. The following case study of electric power and natural gas interdependencies in Florida further illustrates this point. Because Florida is a terminal state, this case study represents one of the simplest examples

of interactions between electric power and natural gas because there is no complex downstream system to consider that could further propagate the disruption. Furthermore, the natural gas system is relatively simple with only two major high-pressure transmission pipelines serving the state (i.e., Florida Gas Transmission Co. and Gulfstream Natural Gas System). Figure 07. Cascading Failure Simulation in Florida shows the results of the cascading failure simulation between natural gas and electric distribution systems in Florida.

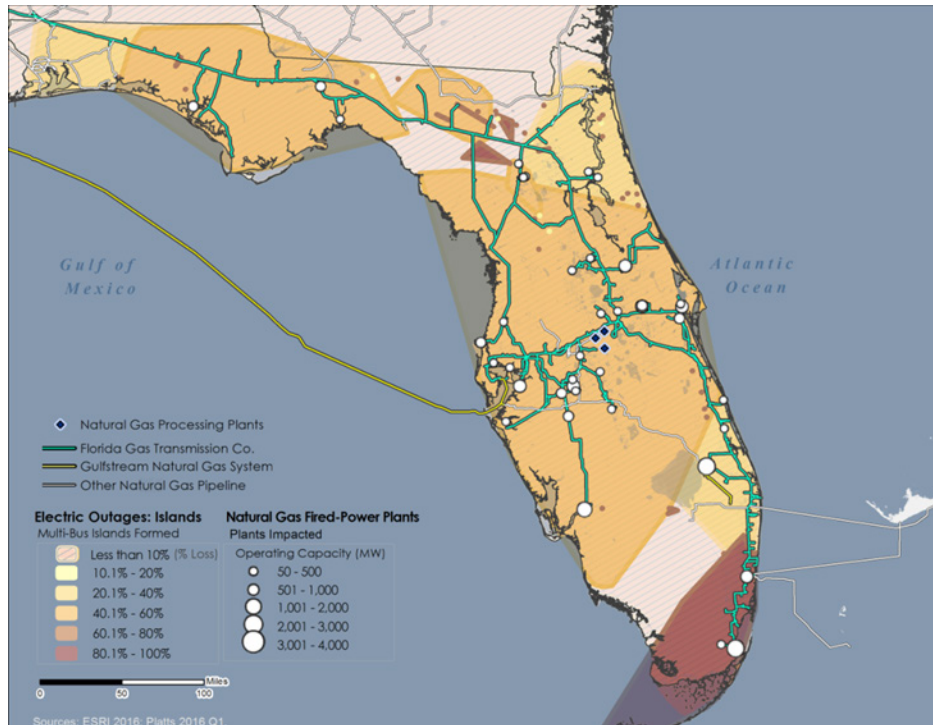


Figure 07. Cascading Failure Simulation in Florida

The scenario postulates the occurrence of a guillotine (i.e., complete) break on a major interstate transmission pipeline supplying natural gas to the state, resulting in a 100% reduction in the flow of gas through the pipeline. The pipeline break also disrupts fuel delivery to a large number of gas-fired power plants in the state. These power plants would cease operation, leading to a statewide electricity outage with varying load curtailment intensity ranging from 10% to 100%.⁵

In addition, the scenario assumed that Florida has three small natural gas processing plants located in an area that would experience a 40% percent load curtailment, requiring them to curtail operations temporarily. However, because the combined output from these facilities is small relative to the total load, the associated gas curtailment would have no notable impact on gas customers in Florida.⁶

As discussed in the previous section, infrastructure failures are not all created equal. When interdependencies are involved, a failure in one infrastructure can cascade to other systems increasing the overall consequences. Therefore, considering interdependencies should be an integral part of critical infrastructure security and resilience programs.

Applying an Optimization Algorithm to Prioritize Infrastructure

Managing risk associated with infrastructure interdependencies requires an understanding of infrastructure failures and, especially in complex urban environments, an ability to prioritize protection and mitigation efforts. Argonne has developed an optimization algorithm for selection and prioritization of infrastructure that runs at the system-level or the interdependent “system of systems-level”. The algorithm can apply to the assessment of any infrastructure system.

The optimization algorithm assumes that the physical behavior of a system (e.g., a power network, gas pipeline, or coupled system) is described by the following optimization problem:

$$F(d) := \min_{u \in U(d)} f(u)$$

where:

d is the 0-1 vector representing the failures at infrastructure assets,

u is the control(s) that can be manipulated to mitigate disturbances, and

$f(u)$ is a system output metric of interest such as cost, delivered load, or deviations from a target operation.

This problem can be solved by the generalized Benders decomposition method proposed by Salmeron *et al.* (2009).⁷ This method solves the master problem $\max_{d \in D} F(d)$ by iteratively approximating the function $F(d)$ with a set of linear inequalities. Set D contains a set of failure scenarios denoted by d . An element of the set D is denoted by $d = (d_1, d_2, \dots, d_n)$, where an element d_i of the vector is either 0 or 1 for $i = 1, \dots, n$ to create a combination of the asset states. For example, $d = (0,0,1,0)$ can model an event in which, out of $n = 4$ assets, the third asset is disrupted whereas the other assets are not.

The dependence of the control set $U(d)$ on d captures the fact that the control actions available to counteract the disruption might be affected by the disruption d . The control set implicitly captures the network topology and physical laws of an infrastructure system.

Worst-case contingency analysis aims to find a contingency that causes the maximum damage to the system. The worst-case event (denoted by $d^{(1)}$) can be found by solving the optimization problem:

$$D(1) = \operatorname{argmax}_{d \in D} \min_{u \in U(d)} f(u)$$

The second most damaging event (denoted by $d^{(2)}$) can be identified by restricting the event set as $D \setminus \{d^{(1)}\}$ and by solving the problem $d^{(2)} = \operatorname{argmax}_{d \in D \setminus \{d^{(1)}\}} \min_{u \in U(d)} f(u)$. This procedure can be applied recursively to identify the k -th most damaging disturbance. This step is performed by restricting the disturbance set as $D \setminus \{d^{(1)}, d^{(2)}, \dots, d^{(k-1)}\}$. Our optimization algorithm systematically restricts the disturbance set by iteratively adding the linear inequalities to the

worst-case interdiction problem. This approach significantly saves the computational times, as compared with an exhaustive search.

The algorithmic steps are then summarized for identifying the most damaging disturbances as follows:

1. Create the initial set of disturbances D and the control set $U(d)$ that is dependent on disturbance $d \in D$. Set $k = 1$.
2. Solve the worst-case interdiction problem to find $d(k) = \operatorname{armax}_{d \in D} \min_{u \in U(d)} f(u)$.
3. If $k = K$, then **STOP**.
4. Update the disturbance set in order to exclude the k -th most damaging disturbance $d^{(k)}$.
5. Update $k = k + 1$, and go to step 2.

In step 2 of this algorithm, updating the disturbance set (step 4) is also equivalent to adding a linear constraint to the Benders master problem. The optimization algorithm has been implemented in Julia script language, and CPLEX is used to solve the master and subproblems in the generalized Benders decomposition.

Argonne has applied this optimization algorithm to a test system of the California Independent System Operator (CAISO) interconnected with the Western Electricity Coordinating Council (WECC). The test system is obtained from Kim *et al.* (2017).⁸ This test system consists of 225 buses, 375 transmission lines, 135 generation units, and 40 loads.⁹ The algorithm ran to detect the 100 most critical substations in the system. The criticality of substations is measured based on the amount of load lost resulting from the event that a substation is disabled. In this computational test, the objective function $f(u)$ is defined as the amount of load lost. The control set $U(d)$ is defined by a set of constraints for the security-constrained economic dispatch problem as in Kim *et al.* (2017).¹⁰ Note, however, that our algorithmic approach is generic to have a user-defined objective function and additional constraints (e.g., generation cost, repair time of the failure components etc.). Figure 8 shows the results based on the test system.

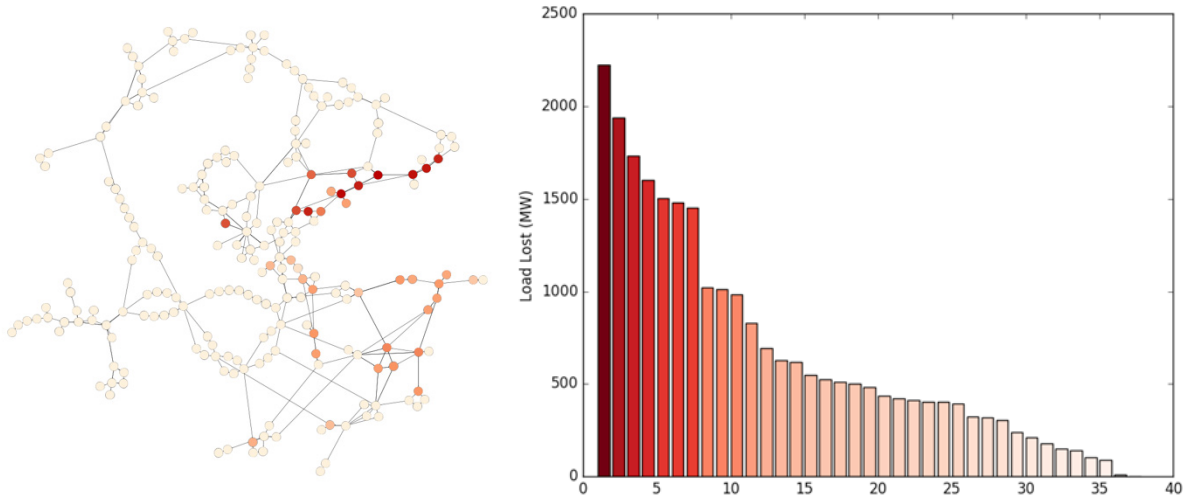


Figure 8. Result of the Optimization Algorithm for the Test System of CAISO Interconnected with the WECC

In this example, a total of 36 substations resulted in significant load loss and failures; the other substations did not cause any load loss. The optimization algorithm terminated after the detection of zero-load substation failure. Government analysts and infrastructure owners and operators can use this type of information to protect the highest consequence failure points within infrastructure systems.

Conclusion

Protecting critical infrastructure, especially in complex urban areas, should focus on identifying and prioritizing potential failure points that would have the most severe consequences. Applying a technique like this optimization algorithm can inform this prioritization process. For example, the algorithm can identify the highest-consequence failures resulting from a cyber-attack against a specific critical infrastructure system, or identify the most consequential failures affecting complex interdependent infrastructure systems supporting a large urban area, regardless of the cause of disruption. Infrastructure system owners and operators, and government agencies can use results from optimization modeling to identify priority assets for in-depth security and resilience assessments, and to inform investment decisions related to critical infrastructure protection and mitigation.

Argonne is currently refining the optimization algorithm framework described within this paper through the Resilient Infrastructure Initiative, which is funded through Laboratory Directed Research and Development (LDRD) resources.¹¹ The list of critical assets resulting from the optimization algorithm can be analyzed further by infrastructure impact models such as EPfast¹² for electric power. Because of the computational complexity of assessing high numbers of infrastructure connections and associated failure scenarios, these studies are performed on Blues, a 350-node, high-performance computing cluster at Argonne.

About the Authors

Duane Verner is the Resilience Analysis Group Leader within the Global Security Sciences Division at Argonne National Laboratory. He oversees staffing and technical assignments, including critical infrastructure vulnerability assessments, modeling, and dependency analyses. He has provided methodology development and project implementation support to the U.S. Department of Homeland Security Regional Resiliency Assessment Program since its inception in 2009. Duane is vice-chair of the National Academies Transportation Research Board's (TRB) Committee on Critical Transportation Infrastructure Protection and a member of the TRB Military Transportation Committee. He regularly contributes to the international resilience research community through publications and trans-Atlantic collaboration. Prior to his position with Argonne, he was a project manager for a private sector engineering firm in New York City, working in the transportation, homeland security, and defense sectors. He may be reached at dverner@anl.gov

Frédéric Petit is a Research Scientist specializing in critical infrastructure interdependencies and resilience at Argonne National Laboratory. With a background in earth sciences and civil engineering, Dr. Petit has focused on risk management and business continuity since 2002. Dr. Petit leads the development of methodologies for the assessment of preparedness, mitigation, response, recovery, and overall resilience capabilities of facilities, communities, and regions. He also lends his expertise to work on risk, vulnerability and threat analysis of critical infrastructure. Dr. Petit received his PhD from the École Polytechnique de Montreal in Civil Engineering, focusing on vulnerability analysis techniques for critical infrastructure cyber dependencies. Dr. Petit is member of various program committees for conferences, such as the Symposium on Risk Management and Cyber-Informatics (RMCI) and the National Symposium on Resilient Critical Infrastructure. He serves as Regional Director for North America of the International Association of Critical Infrastructure Protection Professionals (IACIPP) and is member of the International Advisory Board for the SmartResilience Project. He may be reached at fpetit@anl.gov

Kibaek Kim is an assistant computational mathematician in the Mathematics and Computer Science Division at Argonne National Laboratory. He holds Ph.D. and M.S. degrees from Northwestern University and a B.S. degree from Inha University in Korea, all in industrial engineering. He currently serves as a reviewer for several peer-reviewed journals, including *Operations Research*, *Mathematical Programming*, *Computational Optimization and Applications*, *European Journal of Operational Research*, and *IEEE Transactions on Power Systems*. His research interests are in modeling and parallel algorithms for large-scale optimization problems in applications to network design, planning, and operations. He may be reached at kimk@anl.gov

Acknowledgment

The work presented in this paper was partially supported by Argonne National Laboratory under U.S. Department of Energy contract number DE-AC02-06CH11357. The submitted manuscript has been created by UChicago Argonne, LLC, Operator of Argonne National Laboratory ("Argonne"). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself,

and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

If you would like more information regarding this paper, please contact Duane Verner at dverner@anl.gov.

Notes

- 1 The percentages represent the line transfer capabilities.
- 2 About 5% of power is lost during transmission because of energy dissipated in the conductors and the equipment used for transmission. Thus, from a starting generation capability of 1,520 MW, a maximum of about 1,450 MW of power arrives at the substation. For the purpose of illustration, the example assumes that electric power is divided equally among the transmission circuits that remain operable.
- 3 For the purposes of illustration, the example assumes that electric power is divided equally among the transmission circuits that remain operable. In a real case, it would be expected that Corridor 2 would operate at higher capacity to compensate.
- 4 Adapted from J. Phillips, et al. , *State Energy Resilience Framework*, Argonne National Laboratory, Global Security Sciences Division, (2016) ANL/GSS-16/4, Argonne, Ill, USA, available at <https://www.energy.gov/sites/prod/files/2017/01/f34/State%20Energy%20Resilience%20Framework.pdf>, accessed February 14, 2017.
- 5 E. Portante et al. , "Modeling Electric Power and Natural Gas Systems Interdependencies," *The CIP Report*, Center for Infrastructure Protection and Homeland Security, George Mason University School of Law, Washington, D.C., USA, May–June 2016, available at <http://cip.gmu.edu/2016/06/03/modeling-electric-power-natural-gas-systems-interdependencies/>, accessed February 14, 2017.
- 6 Ibid.
- 7 J. Salmeron, K. Wood, and R. Baldick, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids," *IEEE Transactions on Power Systems* 24.1: (2009) 96–104.
- 8 Kibaek Kim, et al., "Data Centers as Dispatchable Loads to Harness Stranded Power," *IEEE Transactions on Sustainable Energy* 8.1 (2017): 208-218.
- 9 Ibid.
- 10 Ibid.
- 11 Argonne Energy and Global Security, undated, *Resilient Infrastructure*, available at <https://www.anl.gov/egs/group/resilient-infrastructure>, accessed February 14, 2017.
- 12 E.C Portante et al., "EPfast: A Model for Simulating Uncontrolled Islanding in Large Power Systems," *Proceedings of the Winter Simulation Conference*, 2011 Winter Simulation Conference.

Copyright © 2017 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, Resilience, and “Antifragility”

By Eric F. Taquechel and Ted G. Lewis



Abstract

How is the theory behind critical infrastructure/key resources (CIKR) protection evolving? Practitioners who implement strategies should be confident their strategies are based on sound theory, but theory evolves just as strategy evolves. Many theories, techniques, and models/simulations for CIKR protection have been proposed and developed over the years. This paper summarizes several of these approaches and explains how they relate to basic risk concepts explained in the Department of Homeland Security (DHS) Risk Lexicon.

We explain unique contributions of ways to model threat, vulnerability, and consequence, which have implications for how we assess risk. This work builds on previous work in the areas of operations research, prospect theory, network science, normal accident theory, and actuarial science. More specifically, we focus on deterrence measurement to characterize threat differently. We also explain work that models supply chains or “transfer pathways” as networks and applies principles of reliability engineering and network science to characterize vulnerability differently. Next, we explain work to incorporate CIKR resilience and exceedence probability measurement techniques to characterize consequence differently. Finally, we conclude with implications of how CIKR risk may be treated.

We anchor our exposition of these contributions with various terms from the DHS Risk Lexicon. Also, we present these ideas within a framework of three “attack paradigms”: direct attacks against a single CIKR with the intent to destroy just that target, direct attacks against a single CIKR with the intent to disrupt a system of infrastructure, and exploiting CIKR to move a weapon of mass destruction (WMD) through the global commons to its ultimate destination.

Suggested Citation

Tauechel , Eric F., and Ted G. Lewis. “A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, Resilience, and “Antifragility.” *Homeland Security Affairs* 13, Article 8 (October 2017). <https://www.hsaj.org/articles/14087>

Introduction

A strategy for critical infrastructure and key resource (CIKR) protection should have solid theoretical underpinnings. How is theory regarding CIKR protection evolving? Practitioners who implement strategies should be confident their strategies are based on sound theory, but theory evolves just as strategy evolves.

Many theories supporting CIKR protection and resilience have been proposed for application or repackaged into new theoretical approaches. This paper will focus on recently proposed theoretical approaches to protecting CIKR from terrorism and other threats, summarizing the authors’ work in several realms of CIKR protection, and incorporating other insights. Importantly, the authors’ work in these domains builds on rich foundations of previous work in the risk analysis, network science, reliability engineering, and operations research (OR)

fields. This paper will minimize technical discussions of each individual theoretical approach, and instead will propose how these approaches fit together to support implementation of the basic Department of Homeland Security (DHS) risk equation Risk = Threat x Vulnerability x Consequence. Also, we will anchor our exposition of these approaches with other terms from the DHS Risk Lexicon (hereafter "Lexicon").

This basic equation still forms the DHS foundation for CIKR risk analysis and mitigation, although there are different opinions in the literature on the appropriate ways to characterize the finer details of the equation's components and how data is collected and analyzed.

Background: Current State

The Lexicon defines risk as the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences."¹ Likelihood is:

"the chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities."²

And, consequence is:

"the effect of an event, incident, or occurrence, including human consequence, economic consequence, mission consequence, psychological consequence."³

So, what are considerations for estimating the chance of a terrorist attack on a CIKR being attempted or succeeding, and what are considerations for evaluating effects of an attack on CIKR? We now examine context for threat and vulnerability, the combination of which form the chance of successful execution of an attack. We also examine context for consequence and resilience.

Context: Threat

Threat is the likelihood that an attack occurs, and that likelihood includes attacker intent and attacker capability, estimated as probabilities. Ordinarily, threat is an input to the DHS risk equation. However, there is a body of literature in the OR world that expresses concerns with treating threat as an input to the equation, instead advocating it should be an output. This is because terrorists, as thinking adversaries, can adapt to our defenses. For example, see Cox (2008)⁴. If this is true, then intent, expressed as a probability an attack is desired, is not necessarily constant. In that case, the quantification of risk would be inconsistent. Instead, those in the OR field have suggested that threat should be an output of vulnerability * consequence, signifying that prospective attackers formulate intent to attack based on observations and estimates of specific CIKR vulnerability and consequence.

Deterrence: Influencing Attacker Intent

The Lexicon defines deterrence as a “measure that discourages, complicates, or delays an adversary’s action or occurrence by instilling fear, doubt, or anxiety.”⁵ Historical literature on deterrence theory and studies of deterrence theory in action tend to focus on what we refer to as “absolute deterrence”: influencing an opponent’s decision calculus such that they decide not to act. However, we think the concept of “relative deterrence” in CIKR threat and deterrence analysis warrants consideration. The probability of acting in a certain manner may constitute a metric for relative deterrence, as opposed to either acting or not acting.

Game Theory and Deterrence

Game theory has been applied to economics and other fields to model interactions and expected outcomes. It models the interactions of intelligent agents, often quantitatively so. It has also been applied to explain nation-state conflicts. In recent work it has been used in counterterrorism modeling. For example, see Yin et al. (2010) who apply game theory to develop an “intelligently randomized” homeland security boat patrol model for the U.S. Coast Guard.⁶ The particular approach that Yin et al. develop leverages the concept of a Strong Stackelberg Equilibrium (SSE) to model how an attacker can observe a defender’s defenses and then pick their best course of action, e.g. attack the CIKR that is the best combination of minimally defended and most valuable to attack. One can link the claim that threat should be an output of a risk equation to the attribute of game theoretic modeling that yields preferences as outcomes of strategic interactions. For example, a “mixed strategy” reflects probabilistic preferences of intelligent agents. Evaluating these probabilistic preferences may lay the foundation for making claims of “relative deterrence”.

The Weapon of Mass Destruction (WMD) Threat

There is also a repository of literature that discusses concern over terrorists exploiting the maritime supply chain to move a WMD into the U.S. The DNDO, or Domestic Nuclear Detection Office, was established to help mitigate this threat. Various technological solutions and modeling approaches to reduce WMD risk have been explored.

Context: Vulnerability

Vulnerability is the likelihood an attack is successful, given it is attempted.⁷ Attacks can be against individual CIKR with the intent of destroying those CIKR. A second paradigm is that attacks might occur against individual CIKR with the intent of destroying/damaging a *system* of CIKR. The Lexicon defines a system as:

“any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.”⁸

Similarly, a network is defined as:

“A group of persons or components that share information or interact with each other in order to perform a function.”⁹

If we focus on the vulnerability of *systems* of CIKR to terrorist attack, perhaps our techniques to assess vulnerability should be different than those of the standard individual CIKR vulnerability assessment. Network science offers techniques for assessing vulnerability of systems to perturbation, considering both the vulnerabilities of individual assets, and then characterizing the vulnerability of systems. For examples, see Lewis, 2006, chapter 5,¹⁰ and Lewis, 2009, chapter 11.¹¹ Also, Lewis (2011) defines criticality as the degree of system dependence on a single component. But, the Lexicon focuses on criticality of an asset to its customer base.¹² Perhaps we can stretch the Lexicon definition to mean the “customer base” of an asset could include its linked components that form a system.

A third paradigm for framing vulnerability analysis is that CIKR are susceptible to exploitation for nefarious purposes, such as moving a WMD through a port infrastructure with the intent to detonate in an inland city. Though some CIKR might have great security against direct attacks, they might have suboptimal security for interdicting a WMD being moved through enroute to a different destination.

In sum, we offer three paradigms for modeling attacks:

Paradigm 1: direct attacks against CIKR with intent to disable/destroy that CIKR;

Paradigm 2: direct attacks against CIKR with intent to cause cascading perturbations throughout a system of CIKR; and

Paradigm 3: exploitation of a CIKR to inflict damage on a different CIKR “downstream” in a system.

Context: Consequence and Resilience

We cited the Lexicon definition of consequence earlier. Then, the Lexicon goes on to define resilience as the “ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.”¹³ Thus, to the extent disruptions create undesirable effects or consequences, resilience is the ability to recover from consequences. Vugrin et al. (2010) focus on the magnitude and duration of deviations from desired system performance levels as two parameters of the ability to recover from disruptions.¹⁴

DHS websites on resilience acknowledge the evolution of policy emphasis on resilience towards efforts to define it.¹⁵ However, when we did our research, DHS policies and programs emphasized resilience but did not explicitly guide stakeholders on how to quantify it or how to implement resilience measures. So, it falls to academia to propose definitions.

Evolution: Possible Future States

Given this context, how might theory supporting threat, vulnerability, and consequence analysis evolve? We now summarize our work in these areas.

How We Analyze Threat: The Importance of Deterrence and Cognitive Biases

We mentioned earlier that the concept of “relative deterrence” in CIKR threat and deterrence analysis warrants consideration. Instead of convincing our opponent not to act at all, or conceding they will definitely commit an undesired act, does it make sense to think of influencing attacker intent on a spectrum – in probabilities? In other words, is it worth exploring the probability one attack is quantitatively more desirable than an alternative attack, when multiple CIKR are possible targets? And, should we try to model how attacker intent might change, as a proxy for deterrence?

The game-theoretic modeling approaches discussed earlier leverage algorithms that produce a probability distribution. This probability distribution is translated into a tactical patrol schedule for armed Coast Guard law enforcement boats throughout their area of operational responsibility. In theory, executing their patrol schedules according to this probabilistic distribution minimizes the chances an observant adversary can plan and execute an attack on maritime CIKR. Moreover, in theory this deters an attacker, at least from a “relative deterrence” standpoint.

Starting Simple: Quantifying Deterrence

Given our belief that relative deterrence warranted attention, and given that previous literature had leveraged game theory to produce a probabilistic approach to deterrence, we published a paper entitled “How to Quantify Deterrence and Reduce Critical Infrastructure Risk” in 2012.¹⁶ The thrust of this approach was that deterrence against CIKR attacks can be quantified as the extent to which attacker intent to attack a certain CIKR changes after security measures are implemented at that CIKR, as compared to attacker intent to attack that CIKR before implementation of such measures. The quantification of deterrence took a very simple form:

$$E_l \Big|_k = \frac{Intent_i^{pre} \Big|_{\$AB} - Intent_k^{post} \Big|_l}{Intent_i^{pre} \Big|_{\$AB}}$$

Equation 1. Quantification of deterrence¹⁷

The intent values were based on expected utility ratios of pre-security expected utility from attacking the CIKR in question, and post-security expected utility. These expected utility values were derived from a game theoretical CIKR attack game between a notional attacker and notional defender, such as a CIKR operator.

We claimed that expected utility from an attack should include the quantification of attacker capability as a probability, but should exclude probabilistic expressions of intent.

This was our “compromise” between the default risk equation that incorporates both intent and capability into the threat component, and the Operations Research (OR) community objections to including threat as an input because it fails to account for adaptive adversaries.

Also, we used an exploratory approach to the game theoretical scenario, averaging results of possible courses of action that the notional attacker and defender faced, rather than relying on the theoretical Nash Equilibrium solution of the game. A Nash Equilibrium predicts the “optimal” outcome of a game such that each player will choose the best solution they possibly can, given their opponent is also trying to pick their own best solution. Thus, we hedged for the possibility that an attacker might not necessarily pick the theoretically “optimal” solution.

This work built on a previous thesis which claimed risk propensity, or an actor’s attitude toward risk and choice, should influence deterrence.¹⁸ In our paper, we made the opposite (but possibly complementary) claim: *that deterrence should influence risk analysis*. We also incorporated previous work on modeling vulnerability reduction as an exponential function of dollars invested to improve security; Al-Mannai and Lewis (2008) proposed example functional forms.¹⁹ We treated vulnerability as a linear function of investment, which may have been an oversimplification.

Furthermore, we explored conditional and unconditional risk. Unconditional risk reflected the risk of CIKR attack given the attacker’s intent (as modified by security investments), combined with their capability, vulnerability, and attack consequence. However, conditional risk reflected the equivalent of attacker expected utility: the product of attacker capability, CIKR vulnerability, and CIKR failure consequence. This was consistent with the Lexicon definition of conditional probability: the probability of some event given the occurrence of some other event.²⁰ The “other event” we surmised was the attacker decision to attack a specific CIKR with 100% intent. Thus, we treated conditional risk as the product of capability, vulnerability, and consequence, multiplied by an intent factor of 1.

Finally, we made a case for differentiating tactical intelligence from strategic intelligence in a game theoretical context. Strategic intelligence in some CIKR risk tools at the time of our writing reflected high-level quantitative estimates of various terrorist group intent to attack certain types of CIKR and capability to use various attack modes. As an alternative, we proposed that tactical level intelligence with regard to CIKR protection entailed a target-specific assessment of vulnerability and consequence by a would-be attacker, both before and after hypothetical security measures were implemented. This tactical intelligence would reflect their target-specific intent to attack (or not attack), and when compared to their estimated intent to attack other CIKR, could be leveraged to estimate unconditional risk and create “deterrence portfolios” to characterize various security investment options and inform decision makers.

One objection we anticipated when we wrote the paper was that deterrence efforts simply may shift prospective attackers to other CIKR with higher consequence. This broached the concept of threat-shifting. The Lexicon defines threat-shifting as the:

“response of adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle.”²¹

The Lexicon then goes into detail about domains in which threat-shifting can occur, including target domain: selecting a less protected target. However, we claimed our approach allowed for threat-shifting, more specifically “intent-shifting”, but did not necessarily increase *risk* to the CIKR in the game.

We applied our methodology to quantify deterrence and measure the change in CIKR risk in a notional case study, with the security investments modeled as hypothetical investments provided by FEMA’s Port Security Grant Program (PSGP).

The Lexicon definition of “adaptive risk” includes:

“threats caused by people that can change their behavior or characteristics in reaction to prevention, protection, response, or recovery measures taken.”²²

By examining and quantifying how adversaries might assess desirability of various CIKR attacks in response to hypothetical protection measures, we add granularity to CIKR risk analysis and make more informed CIKR investment decisions. Furthermore, the Lexicon claims,

“for some types of risk, like those involving human volition, the probability of occurrence of an event may not be independent of the consequences and, in fact, may be a function of the consequences.”²³

In our approach, the probability of *intent*, not of attack occurrence, was modeled as a function of a combination of consequences, attacker capability, and modifications to vulnerability, based on hypothetical grant investments.

Increasing Complexity – Threat, Deterrence and Cognitive Biases

Our work on quantifying deterrence assumed Expected Utility Theory (EUT) applied to the expected utility functions. This theory provides that people make decisions linearly, estimating costs, benefits, and probabilities. They make decisions consistently across how information is provided, or “framed.”

However, Daniel Kahneman and Amos Tversky, Nobel Prize winning psychologists, showed experimentally that people often make decisions inconsistently depending on changes in frame, in contravention to the tenets of EUT. They created Prospect Theory (PT) to explain their findings. Therefore, in a follow-up piece to our work on quantifying deterrence, we modified our approach to account for PT considerations in deterrence. We also explored whether information incompleteness could influence the quantification of deterrence and resulting CIKR risk.

The Lexicon annotates the definition of “social amplification of risk” as follows:

“a field of study that seeks to systematically link the technical assessment of risk with sociological perspectives of risk perception and risk-related behavior.”²⁴

Kahneman and Tversky discovered that people perceived risk differently when prospective outcomes were presented as losses from a reference point, rather than gains beyond that reference point. They modeled the relationship between gain/loss and value as a nonlinear function:

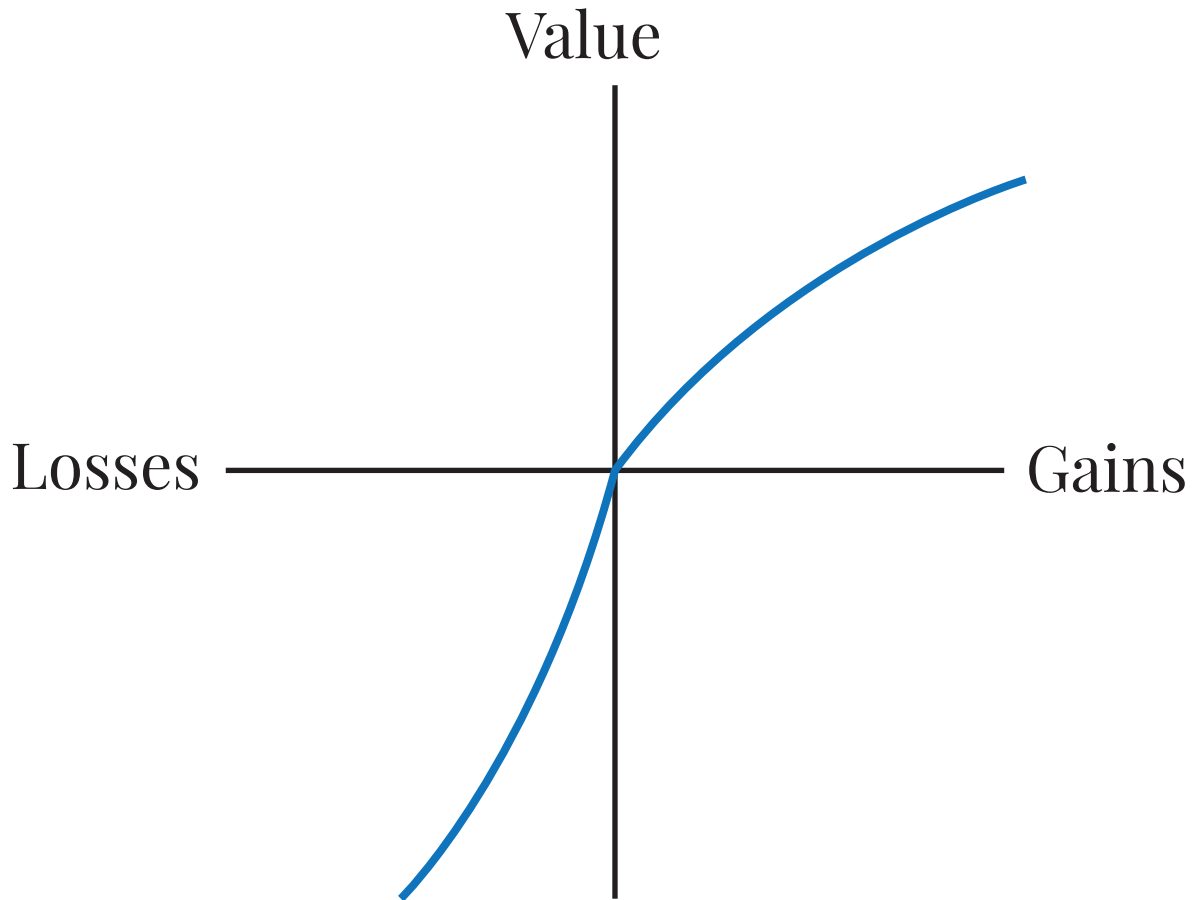


Figure 1. Relationship between gain/loss and value²⁵

Figure 1 reflects their findings that losses held more “value” or salience to those faced with prospects, than did quantitatively equivalent amounts of gain. This finding violated one of the central tenets of EUT. Kahneman and Tversky also discovered a phenomenon they dubbed the “certainty effect” meaning that subjects generally preferred certain outcomes to probabilistic outcomes. When presented with gains, subjects preferred a certain smaller gain to a larger but probabilistic gain. When presented with losses, subjects preferred probabilistic larger losses to certain smaller losses, thus reversing the certainty effect and yielding the term “reflection effect.” Figure 2 below amplifies on comparisons between EUT and PT, although the claims regarding what behavior losses and gains might predict under PT assumptions omit a discussion of probability – both the “certainty effect” and “possibility effect” that Kahneman discusses in his 2011 book, *Thinking Fast and Slow*.²⁶

Utility Theory

		SEU: Asset Position	PU: Reference Point
Risk Propensity	Risk Seeking	Low % of high utility	Overweight utility when presented as loss relative to reference point
		High Certainty Equivalent (CE)	High CE
		Gamble more preferred than expected value for certain	Losses predict risk-seeking
	Risk Averse	High % of low utility	Underweight utility when presented as gain relative to reference point
		Low CE	Low CE
		Gamble less preferred than expected value for certain	Gains predict risk aversion

Figure 2. How EUT (also Subjective Expected Utility or SEU) and Prospect Theory (here called “Prospect Utility”) may influence Risk Propensity²⁷

Thus, we applied insights from their discoveries to predict what would-be CIKR attackers might prefer from amongst various CIKR attack options. The overall goal of this new research was to explain and recommend an approach to support decisions on whether to publicize information about CIKR security investments intended to deter attack, or whether to obfuscate those investments, by considering what we called “cognitive biases”.

First, we proposed a new definition of a “prospect” to distinguish the use of that word from its use in PT. A prospect simply meant the aggregation of possible future outcomes from an attacker COA (course of action). We then further specified that an “ordinary prospect” mean a prospect *not* derived from a game theoretic scenario.

We expanded on these definitions of prospect by then proposing the concept of “equilibrium prospect” meaning a prospect where the outcomes were influenced by what an intelligent opponent might do in a game theoretic interaction. Moreover, we showed what the equation for an ordinary prospect might look like if it was modified based on Kahneman and Tversky’s findings. This equation would reflect a relationship between gains/losses and value ascribed, fitted to the data that Kahneman and Tversky gleaned during their research.

These differentiations in equations for prospects helped us alter the way we proxied attacker intent as we explored how information incompleteness and prospect theory could influence deterrence quantification and resulting risk. For example, one assumption was that an attacker would choose the equilibrium solution to a deterrence game; therefore, their quantified intent for that COA would be 100%. Alternatively, they might hedge among all prospective outcomes of the game, comparing the expected utility of one possible outcome to the aggregate of expected utilities of all possible outcomes, thereby creating an “intent ratio” proxy for their intent. Or, they might choose an “aggregate prospect” with maximum value with 100% probability - reflecting the sum of expected utilities if the attacker chose one COA, but reflecting the aggregate influence of possible defender actions in the game. Finally, they might create intent ratios using prospects, rather than using individual game outcomes.

We also proposed a heuristic for analyzing outcomes of deterrence games under conditions of incomplete information. In this case, the attacker would play a different “game” than the defender, since the attacker created proxies for defender deterrence investments at the CIKR in the game, whereas the defender knew their true investments. We proposed the term “organizational obfuscation bias” or OOB to represent attacker bias under conditions

of incomplete information. We proposed business rules for how to quantify deterrence and create deterrence portfolios under these conditions.

Furthermore, we used an exponential investment-vulnerability relationship as an alternative to the linear relationship from our 2012 paper. Exponential relationships between effort and result may be more realistic than linear relationships, especially in counterterrorism analysis on the assumption our adversaries adapt to observable (or unobservable) vulnerability reduction measures.

Also, in our update we explored the effects of incomplete information. Different authors in the deterrence theory literature suggest different things. Some suggest deterrence is most effective when both parties share a common estimate of the other's intentions (for example, see Moran, 2002²⁸) whereas others suggest ambiguity might actually enhance deterrence (for example, see Chilton and Weaver, 2009).²⁹ Furthermore, the game theory literature distinguishes incomplete information from imperfect information. The former means that if all players can observe opponents' previous moves in the game, they might not know all the rules that define the game. In contrast, imperfect information means that even if players know all the rules of the game, they don't know their opponents' previous moves.

Results of Notional Case Study

We varied our deterrence games to assume the attacker had incomplete information and thus we used proxy values to represent what they might estimate the quantitative values of CIKR vulnerability to be, based on attacker OOB. This yielded results that defender risk was less when investments were obfuscated than when they were publicized, for all attacker OOBs, and assuming EUT. However, this was specific to the assumption that the attacker used an intent ratio for intent proxy, rather than selecting an equilibrium game solution. In circumstances when the attacker was presumed to choose the equilibrium solution and intent was thus 100%, there was no quantifiable advantage of obfuscating deterrence investments over publicizing them, again under EUT assumptions. Quantifiable advantage here meant that unconditional risk was lower after change in intent was applied. We also found that if we assumed PT held rather than EUT, the defender gained no quantifiable advantage of obfuscating deterrence investments, over publicizing them.

Together, biases from PT and biases from incomplete information formed our "cognitive biases." The implications of our findings were that under circumstances where it would be quantitatively more advantageous to obfuscate details of possible deterrence investments, the government would also have to obfuscate other details such as available budgets and estimated reduced CIKR vulnerabilities after deterrence investments were made. We therefore expanded upon our 2012 paper claim:

"In order to generalize these findings, any advantage of a specific information availability circumstance must be robust given utility theory assumptions."³⁰

To conclude our discussion on the evolution of how threat can be treated in CIKR risk analysis, we return to the Lexicon which states that risk reduction "can be accomplished by reducing vulnerability and/or consequences."³¹ However, based on our research, we propose that threat reduction, through deterrence quantification and consideration of cognitive biases, may be another way to analyze risk reduction.

How We Analyze Vulnerability: Systems Approaches and Organic vs Inherited Vulnerability, Or Exploitation Susceptibility

Starting Simple – Transfer Threat Modeling

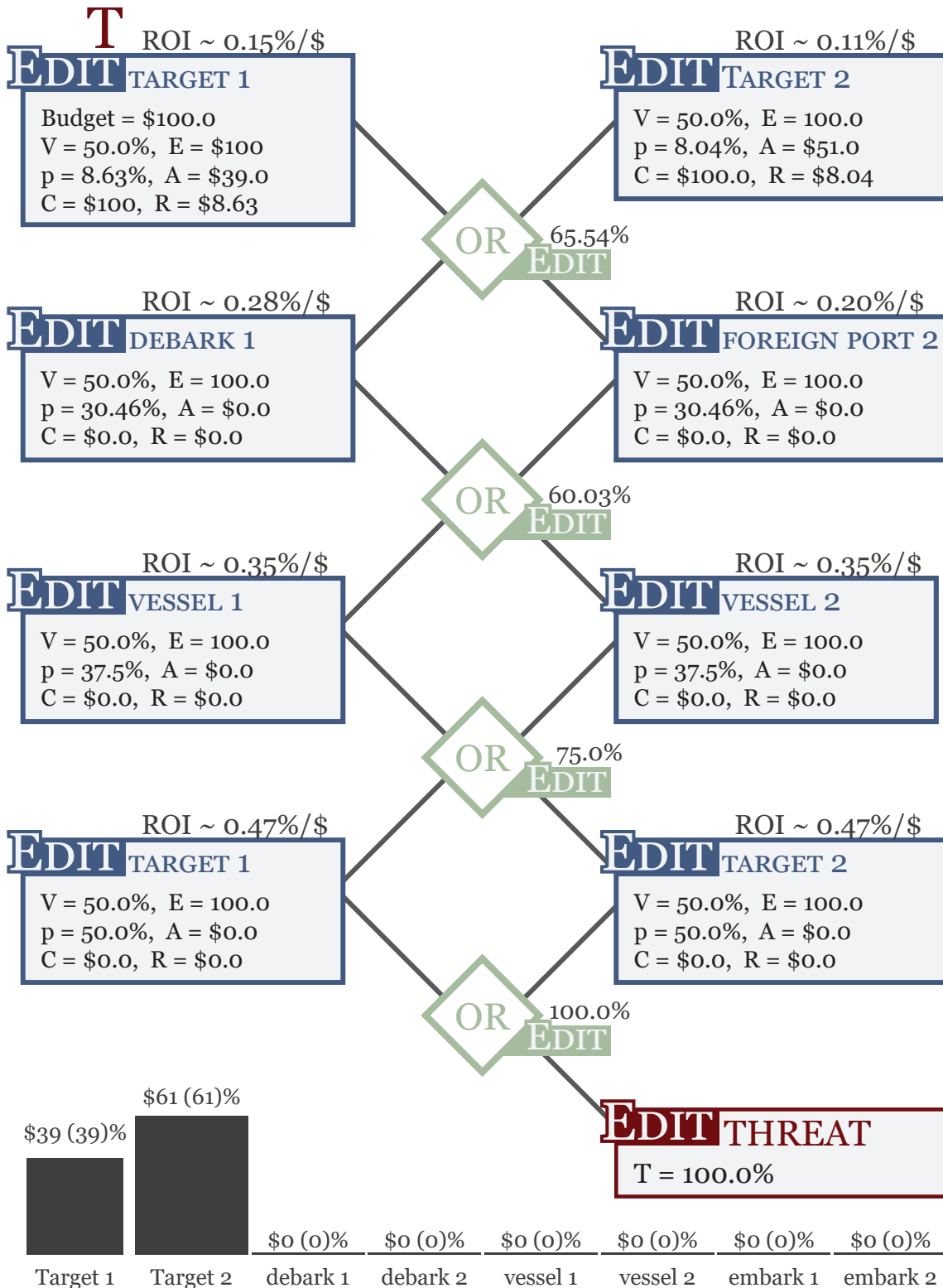
Our first approach to exploring vulnerability in a new light involved the third paradigm we offered for modeling attacks. We explored how to model the concept of “layered defense” for defending CIKR networks from exploitation. Previous work on CIKR protection had leveraged the concept of fault trees.³² Fault trees showed how a fault, or in the case of CIKR risk analysis, a terrorist attack, could propagate throughout a network of CIKR. The Lexicon annotates a fault tree as a tool to estimate quantitatively the probability of program or system failure by visually displaying and evaluating failure paths.³³

However, fault trees only demonstrated what Tauechel (2010) described as “inherited vulnerability” or the probability of fault propagation as governed by De Morgan’s Law and the logic gates (AND or OR) that connected nodes in the fault tree network. In reality, nodes in a CIKR network also have “organic vulnerability” as reflected by their own inherent security measures, or lack thereof.³⁴

Thus, Tauechel reasoned that risk of exploiting a network composed of nodes that had organic security measures must be assessed using a combination of organic and inherited vulnerability terms. For example, a “terrorist transfer network” of overseas and U.S. ports could be rendered as a network of CIKR nodes, with logic gates governing the propagation of illicit material between nodes, but with each node having a quantifiable organic vulnerability inversely proportional to security measures at the node. Returning to the proposed definitions of criticality, perhaps exploitation of this network would depend highly upon one very vulnerable foreign port. Alternatively, it might depend on a more holistic measure of aggregated network failure probability derived from the combination of organic node vulnerabilities and inherited vulnerability of each “layer” of nodes, ports in this case.

Ultimately, we modified Lewis’ Model Based Risk Assessment (MBRA) network modeling tool to create a logic graph that leveraged fault tree principles, but added an emergence-based algorithm to optimize funding to “harden” ports against terrorist transfer, reducing organic vulnerability and thus reducing overall network vulnerability. We combined the concept of topology from network science with the classic CIKR risk analysis treatment of vulnerability. Topology is a “mapping function” showing the relationship between nodes and links in a network.³⁵ It is the “architecture” of the network, which may change over time if the network is “dynamic.”³⁶

Logic gates in this approach reflected a different type of topology, wherein they represented virtual links between nodes, rather than physical links. The virtual link was a proxy for attacker decision making – whether to transfer illicit materials or people through both nodes to get to the next node (AND gate), or to transfer materials through a single node (OR gate). This extended the existing functionality of the MBRA tool to address a problem of interest to DHS as depicted in figure 3.



Allocated = \$100, Likelihood = 16.67%, Risk = \$16.67, Model: Exponential, #Iterations: 332, Step Size = 1.0, No Layers Budget-to-Risk: \$76.27 (Risk = \$8.63), No Layers Risk-to-Budget: \$5.00 (Budget = \$100)

Figure 3. MBRA adaptation logic graph: optimal budget allocation minimizes network risk³⁷

Preferential attachment undergirds the MBRA algorithm we used to model terrorist transfer networks as depicted in Figure 1. Lewis discusses how preferential attachment is a source of Self-Organized-Criticality (SOC), meaning a system is on the verge of collapse due to emergent processes occurring within the system to make it more efficient during steady state functioning, but also more susceptible to failure.³⁸ Essentially, the MBRA algorithm is an emergent algorithm that allocates a dollar to a node to reduce organic vulnerability (or exploitation susceptibility). It documents the reduction in overall system vulnerability and risk. Then, it allocates another dollar at random. If the overall system risk is reduced, the dollars remain allocated as such. The algorithm reflects the system's "preference" for allocations that reduce overall risk or increase overall system resilience. However, if the risk does not change or is increased, the algorithm "retrieves" the previously allocated dollar and searches for another recipient node. This is similar to how ants or termites "self-organize" in their flocking behavior as discussed in Lewis (2011).³⁹

Increasing Complexity – WMD Transfer Modeling

With this third paradigm in mind, our initial work treated terrorist transfer threat as a general threat in our layered defense modeling. However, we decided to then focus more specifically on the WMD (weapon of mass destruction) threat for follow-on work. We also decided to merge our concepts of layered defense and deterrence measurement with a network science approach in our 2015 paper on measuring the deterrence value of securing maritime security chains against the WMD threat.⁴⁰

In this work, we modeled a supply chain that an adversary might try to exploit by transferring a WMD, but we explicitly modeled port "node" vulnerability, or exploitation susceptibility, as a function of notional WMD detection technology in those ports. We modeled probabilities of encounter and detection at notional U.S. ports of debarkation or ports of entry, holding encounter probabilities constant and modifying detection probabilities proportional to the investment necessary to build and operate detection technology. The "elimination fraction" would represent a 95% probability of detecting a WMD within a container in a U.S. port, and the "elimination cost" would represent the investment necessary to build and operate technology with that 95% detection probability. The detection probability was combined with the encounter probability in a U.S. port to produce a notional "organic failure susceptibility" of that port.

Then, we incorporated logic gate principles from the previous layered defense modeling work to proxy attacker "transfer pathways" from foreign ports, through U.S. ports, and ultimately to inland "target cities". These transfer pathways thus represented "inherited exploitation susceptibility", as opposed to inherited vulnerability from previous work. Conceptually, this combined technology effectiveness modeling with network theory and is depicted in figure 4.

We then incorporated concepts from deterrence quantification. Once we could characterize the organic exploitation susceptibility of a port, and incorporate inherited exploitation susceptibility probabilities from logic gates representing transfer pathways, we then could create risk equations, reflecting risk of WMD detonation in a U.S. inland city. These were conditional risk equations that excluded attacker intent probabilities.

These conditional risk equations could change based on the different permutations of transfer pathways an adversary could exploit to transfer a WMD. We converted the equations to utility functions, showing the expected utility an adversary would gain from detonation

of a WMD. Doing so allowed us to then create a game theoretic scenario case study wherein the defender had different options to invest in WMD detection technology equipment at U.S. ports, and the attacker had various pathways to exploit. From this game we gleaned proxies for attacker intent, here again an output of risk equations, and created unconditional risk equations for the inland cities. This created a different flavor of “deterrence portfolio” from the portfolios we had created that reflected attacker intent for direct attacks on CIKR in our 2012 work on quantifying deterrence. This allowed us to measure how various investments in WMD detection technology might deter adversary exploitation of supply chains.

Overall, this work offered an alternative to a claim in the Maritime Commerce Security Plan: that inspecting containers for WMD once they arrive in U.S. ports is too late.⁴² We suggested that this is not necessarily true if the target is an inland city – after the container is offloaded onto a truck and moved toward a large inland population center. However, we did *not* claim that it was altogether imprudent to first inspect containers overseas or at U.S. ports of entry.

Results of Notional Case Study

One finding of our case study that applied our methodology was that the best investment in WMD detection technology was against a specific transfer pathway that differed from what traditional attacker-defender modeling efforts might suggest. This was because our methodology did not necessarily rely on the equilibrium output of the deterrence game we analyzed, but instead hedged against the possibility that an adversary might not consider an “optimal” transfer pathway to exploit.

Another finding was that we could put discussion of possible attacker tactics to move WMD into the U.S. into quantitative terms. If a logic gate between a foreign port and a U.S. port was “AND”, this represented that the vessel the WMD was secreted upon would stop at two foreign ports before its voyage to the U.S. If the logic gate in our model was “OR”, this meant the vessel only stopped at one foreign port before its voyage to a U.S. port.

Similarly, an AND gate between the U.S. port node “layer” and target inland U.S. city meant that the attacker intended to “decentralize” the introduction of the WMD by offloading component parts at one U.S. port. Then, the vessel would continue onto another U.S. port and offload the remaining components. Eventually the attacker would arrange for the components to be reunited and continue their transit toward the inland target city. Alternatively, the OR gate would mean the weapon was moved through a US port of debarkation intact and ready to detonate upon arrival at the target city.

A practical implication of this research was that intelligence collection and analysis efforts might focus on attacker preferences for exploiting various US ports. This would help inform decisions on how to invest in WMD detection technology, accounting for foreign port exploitation preferences. To elaborate, if intelligence estimates were confident that multiple US ports would be exploited in a WMD component “decentralized introduction” effort, foreign port exploitation preferences would be not be especially valuable in informing investment decisions, per the model’s approach.

Another practical implication was that the costs to create WMD detection technology could be compared to the probabilistic effectiveness of detection, to calibrate a model that compared actual investment to “desirable investment” to maximize detection probabilities.

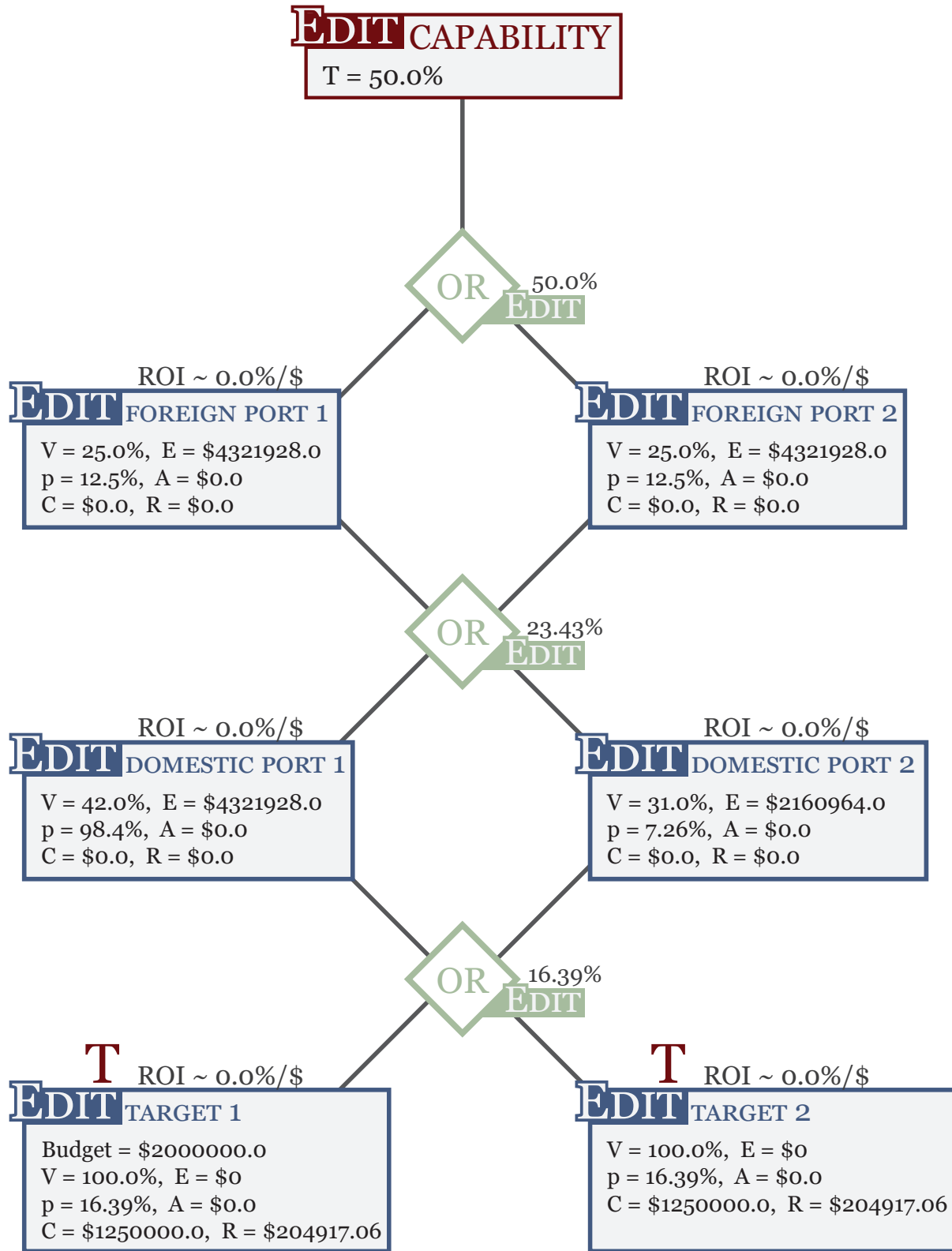


Figure 4. Notional MBRA WMD transfer network⁴¹

The Lexicon claims that event trees are used to project forward in time, modeling probabilities of events leading to some future outcome, whereas fault trees look retrospectively at the cause of an event that has already occurred.⁴³ Fault trees leverage logic gates to combine probabilities. Even though fault trees are recommended for retrospective analysis in the Lexicon, we offer that leveraging logic gates as proxies for attacker decision making and thus leveraging the fault tree approach might be a useful alternative for estimating probabilities of future terrorist attacks.

How We Analyze Consequence: Resilience, Exceedence Probability, Antifragility

Resilience

The Lexicon defines resilience as the:

“ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss.”⁴⁴

With this in mind, we refocused our attention on FEMA's Port Security Grant Program (PSGP). Tauechel had worked in an office that provided technical expertise on port security to FEMA, and thus developed a technical approach to model grant allocation based on a resilience-oriented, network-focused framework. This approach was touted as one option to support a prospective policy decision to convert the PSGP program to a resilience-based program.

Starting Simple – Networks and Resilience

Returning again to the concept of criticality, we claimed maritime supply chains could be modeled as nodes, here ports and inland cities, and links, here means of transportation between those ports/cities. We wanted to show that supply chains might depend on ports to keep running after a disruption, and proposed an approach to reduce the criticality of the ports to the overall supply chain, thereby increasing supply chain network resilience. Resilience funding allocations would reduce the cascading economic disruption effects caused by port shutdown or damage to port facilities.

First, we discussed the idea that we should identify a certain level of supply chain loss to be expected after an attack, but identified challenges with port facilities sharing specific data, for fear of violating proprietary data restrictions or disclosing information that would give their competitors an advantage.

Then we claimed the current theoretical foundation underpinning the FEMA allocation of grant funding, the classic $R=TVC$ equation, might be insufficient if the grant program transitioned to a resilience-based, network-focused approach. This was because this equation did not capture network metrics such as node degree (number of links to other nodes), and instead

took an asset-centric focus on risk, rather than a network-based focus on system resilience. Equation 2 below is a risk equation that accounts for node degree, thus incorporating a network metric:

$$\sum_i R = T \sum_i g VC$$

Equation 2. Risk equation for risk to network with i nodes, g =node degree. Threat (T) is generic threat to network.⁴⁵

We also discussed an approach to modeling system resilience that used network interdiction methods, an approach espoused in the OR community, and explained the difference between those models and probabilistic risk-based network science models.

Next, we proposed definitions of quantifiable resilience for both individual maritime supply chain networks and ports, because our modeling approach leveraged quantitative values of risk, thus linking risk and resilience. We also needed our approach to remain fairly consistent with the PSGP principle of allocating money to ports, and then the ports redistributing money to various claimants such as port CIKR. We further proposed that resilience can be organic and maximized with organic CIKR resources, or enhanced/further maximized with PSGP allocations earmarked to rebuild damages after an attack. Enhanced resilience can be further broken down into mathematically optimal or sub-optimal resilience, depending on decision maker preferences for funds allocation.

Our approach integrated aspects of OR “reverse-engineering”, but in a way we did not discover during our literature review. Instead of reverse-engineering systems to fine-tune performance for steady state operations, our approach would arguably help reverse-engineer maritime supply chain network “performance potential” to return to standards after a perturbation. Also, we proposed how the network science concept of preferential attachment, wherein hubs accumulate increasingly more links to other nodes based on efficiency and optimization of function, can be counteracted by a different “preferential attachment” – the optimization of grant funding towards the most critical hubs to minimize port failure after a perturbation and thus maximize supply chain resilience. The “counteracting” preferential attachment demonstrated during a simulated distribution of resilience funding to network nodes would reduce the economic efficiency-driven SOC that had naturally evolved in that supply chain network.

Throughout our detailed explanation of our model’s equations, we used the phrases “organic failure susceptibility” and “inherited failure susceptibility” instead of “organic vulnerability” and “inherited vulnerability.” We wanted to emphasize that even though the event that precipitated a supply chain network perturbation might be paradigm 2, direct attack to cause cascading downstream effects, the focus of network resilience modeling was susceptibility to failure after the attack had occurred, not the probability the attack would occur in the first place. Thus, we leveraged an approach from our work on layered defense against a terrorist transfer network, but modified it to accommodate probabilities of failure after an attack had already occurred.

We then formulated detailed equations for supply chain network “expected consequence” that modified maximum consequence by applying the failure susceptibility of the nodes in that network. This approach also incorporated a new way to represent inherited

failure susceptibility: node degree or how many links the supplier node and other nodes had to downstream nodes. Our previous approaches to modeling inherited exploitation susceptibility had treated this probability as a function of attacker preferences as modeled via logic gates.

Organic failure susceptibility was now a function of the probability a CIKR node would fail to resume production after a perturbation, based on reserve raw product, relationships with suppliers, and organic ability to rebuild damaged physical infrastructure onsite. This approach leveraged the Lexicon concept of redundancy:

“additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.”⁴⁶

Then, we created a network conditional risk equation, which excluded attacker intent to attack that network, specifically the maritime port CIKR. Next, we combined network conditional risk values to create a proxy “port conditional risk value”. Fourth, we developed an equation for “port organic resilience” as a function of port conditional risk, and developed “resilience ratios” for each port to govern the first “macro-distribution” of PSGP funding to individual ports. In an approach that was reminiscent of how we converted risk to utility for deterrence and threat analysis, we converted risk to resilience metrics in this approach.

Fifth, we showed how our approach could accommodate flexibility to distribute funding to ports based on unconditional port risk as an alternative to conditional port risk. This leveraged the principle of intent ratios from our work on quantifying deterrence, and changed the formulation of the port organic resilience equation. Sixth, we proposed an equation for supply chain network organic resilience, to help guide “micro-distribution” of PSGP funding or subsequent redistribution to maritime CIKR claimants within each port. Just as port organic resilience can be based on conditional or unconditional port risk, we showed how to model network organic resilience based on conditional or unconditional network risk.

Seventh, we revisited the MBRA iterative emergence-based algorithm to be used to optimize PSGP funding distribution amongst CIKR nodes in each port’s supply chains. The objective function of this algorithm was now to maximize port resilience, enabling us to convert organic port resilience to enhanced port resilience. Importantly, this approach optimized by allocating to multiple CIKR within a port, rather than allocating all resources to the most “attractive” CIKR. Eighth, we explained how this optimization would create enhanced supply chain network resilience as a function of network conditional risk after optimal allocation. We then summed the new network conditional risk values to get port conditional risk after an equilibrium allocation was achieved, and then created a new enhanced port resilience value.

Ultimately, we created an approach to synthesize risk, resilience, network science, performance constraints and tradeoffs, optimization, and quantification of deterrence in a unified modeling/simulation approach to potentially support a paradigm shift in an existing DHS program.

Increasing Complexity - Normal Accident Theory, Self-Organizing Criticality, Topology, Exceedence Probability, and Antifragility

We now return to the concept of self-organized criticality (SOC). SOC reflects the catastrophic failure potential of a tightly coupled system prone to cascading failures. With this in mind, we discuss a related theory. Three key ingredients of Perrow's normal accident theory are (1) two failures in a system coming together in an unexpected way; (2) failures cascade faster if the system is tightly coupled, and (3) systems prone to normal accident theory have "catastrophic potential."⁴⁷ Lewis then goes on to explain how power laws can be used to model unpredictability in systems, and how coupledness of system components can be modeled using network theory.

Topology can also proxy SOC, as discussed earlier. In previous discussions of approaches to characterizing vulnerability, we discussed how logic gates can be a proxy for attacker transfer pathway preferences, and are thus a proxy for network topology. Alternatively, we showed how the degree of supply chain nodes, node degree being another proxy for topology, can influence resilience in the port security grant reallocation approach. Essentially, topology influences the coupledness of systems.

If the topology is such that one hub in a network has many links and other hubs have significantly fewer, that network may be considered "scale-free" and likely has a low resilience exponent and is a high risk system. We will explain resilience exponent later. That is, if the hub fails and transmits the failure throughout its many links to other nodes, or other nodes are cut off from supply, the network fails, possibly catastrophically.

Thus, topology is related to network fragility. One way a network becomes fragile is "link percolation" or accumulation of links at a hub, rendering the system more efficient but also more prone to collapse if the hub fails.⁴⁸ If links percolate at multiple nodes, not just the hub, this may have different implications for network topology, fragility, and SOC.

Network Science Metrics, SOC, and Organic vs Inherited Failure/Exploitation Susceptibility

We can argue that node degree of a network's hub, or node with highest link percolation, is a way to proxy network inherited vulnerability or inherited exploitation susceptibility. Furthermore, we can propose that transfer pathways as a proxy for network topology are also a proxy for inherited failure or inherited exploitation susceptibility of a network. This dyad of "physical links" vs "virtual links" is now further explained.

Transfer Networks – Exploitation Susceptibility

A WMD transfer network has high organic exploitation susceptibility if the WMD detection equipment at its nodes is poor. Coupled with OR gates between nodes, here meaning terrorists prefer to ship the WMD components from one foreign port to one U.S. port of exploitation, thus reducing opportunities for detection, this network would have a high exploitation susceptibility, would be fragile, and thus would have high SOC. The prominence of OR gates as a “virtual link” may have similar effect as physical link percolation, in the sense that many links increase exploitation susceptibility by creating many opportunities to transfer a contagion throughout a network.

Focusing on organic exploitation susceptibility, Lewis suggests it makes sense to protect highly connected hubs to prevent network failure. By increasing security at these hubs, we can reduce organic vulnerability or exploitation susceptibility. Returning to the WMD modeling approach, increasing WMD detection technology capability at foreign ports reduces organic exploitation susceptibility of those ports. If they are “hubs” for U.S. shipments, meaning a preponderance of container ships flow through that foreign port enroute to U.S. ports, improving security should in theory reduce overall network exploitation susceptibility and reduce risk, the inherited susceptibilities notwithstanding.

Also, networks can be “rewired” to reduce self-organized criticality, thus changing inherited failure susceptibility. If a hub has some links removed and re-wired to other nodes, the inherited failure susceptibility of downstream nodes might be lowered. To wit, if the newly “less connected” node fails, subsequent cascading network failure may be less likely or have less impact since fewer nodes depend on the hub. However, we would have to evaluate the flow of a failure throughout the remainder of the network if other nodes now have higher degree.

In the case of a WMD transfer network, if an attacker’s desired transfer pathway to move a WMD is forced to change to a riskier pathway (e.g. the AND logic gate which means multiple ports are exploited, increasing their chances of detection), in effect we have “de-percolated” the network. De-percolation may mean reducing the overall number of links in a network, but here we suggest it could also mean re-wiring links away from a hub, reducing degree of that hub. The parallel argument here is that we have reduced options available to the attacker, the equivalent of an AND gate, forcing them to exploit multiple U.S. ports rather than just one. We have thereby increased chances of detection, the organic node WMD detection capabilities notwithstanding, and arguably have reduced SOC.

Supply Chain Networks – Failure Susceptibility

If a maritime port CIKR has many transportation links leading outward to downstream nodes, it has a high degree. Moreover, if that hub and its links (e.g. rail transport in and out of a refinery) are poorly protected, that poor security is a proxy for high network organic exploitation susceptibility. High organic node failure susceptibility (poor security) but few links (low degree) may not have an overall effect on network resilience.

Also, if there are many AND logic gates between nodes, meaning a node needs the supply of multiple upstream suppliers, not just one, then that proxy for network topology increases the inherited failure susceptibility of the network. Therefore, high hub node organic failure

susceptibility, coupled with a certain network topology of logic gates, may increase overall supply chain network SOC to the point of high likelihood of collapse.

Link Density and Topology?

Is link density a good proxy for network topology, or helpful for estimating SOC of a network? Link density represents the ratio of actual links to possible links in a network.⁴⁹ Many links may mean a contagion (e.g. a container with a WMD) can spread easily through a network, meaning a terrorist organization has many options to move the weapon from one node to another. However, many links might also mean a network is resilient, meaning if one link that moves a commodity to another node fails, other links exist to shoulder the load. So, it may depend on what kind of network we are analyzing.

If we are assessing a WMD transfer network, link density may mean there are many links between nodes, or that terrorists consider attractive many different possible transshipment routes between foreign ports, US ports, and inland cities. Therefore, a transfer network with a high link density might naturally be highly exploitable, or have high inherited exploitation susceptibility, notwithstanding the organic security at individual ports of embarkation and debarkation. This network might be said to have high SOC (unless every individual node is highly organically resistant to exploitation). In contrast, a transfer network with low link density might mean very few of the possible transfer pathways are attractive to a terrorist organization. That network would have low SOC.

However, high link density in a supply chain network such as the one we analyzed in our work on the PSGP and resilience might mean something different. If the port “hub” of the network fails or supplier nodes are damaged, downstream cascading effects might be minimized if there are many links. But this would also require high link security or link resilience. Also, it may not matter how many resilient or redundant links exist in the network if CIKR within the port “hub” are the sole sources of supply in the network, but are damaged. Thus, link density may not be a useful metric to ascertain network SOC in this type of CIKR network.

Other Examples of Organic and Inherited Failure/Exploitation Susceptibility

The organic vs inherited failure/exploitation susceptibility dyad appears in other discussions of SOC. For example, Lewis (2011) discusses how to minimize the spread of disease through analysis of a “social network” of people. Prevention of disease is difficult due to the adaptability of microorganisms in response to the evolution of vaccines.⁵⁰ Therefore, it is difficult to reduce the “organic infection susceptibility”, another way of saying “vulnerability to disease”, of individual humans.

However, the alternative could be to change the topology of the human social network through quarantining measures. This would in effect reduce “inherited infection susceptibility” by increasing the length of the links a disease organism must travel between human “nodes” to propagate the infection. Whereas reduction of the number of links in a network is link depencolation, here one can conceive how increasing the length of links between people

could essentially have the same effect as link de-percolation. Conservation of energy means that longer links take energy from shorter links, requiring more expenditure of energy for a disease to propagate, and thus decreasing the likelihood of sustained infection within a population.⁵¹ The individual ability of each person to fight infection when exposed is less relevant here; if the disease cannot travel, even the weakest person would be immune.

Lewis summarizes his discussion of de-percolating human social networks by claiming that “inoculation is a form of hardening that reduces vulnerability while depercolation is a form of resiliency that reduces consequence.”⁵² Here we expand on that concept and claim an alternative interpretation is that inoculation reduces organic failure susceptibility, while quarantine and isolation (depercolation) is also a hardening that reduces network- inherited failure susceptibility. By making it more difficult for failures to cascade between critical infrastructures, for example by increasing redundant sources of supply for downstream refineries in a petrochemical supply chain network, we might de-percolate CIKR networks through removing or effectively bypassing “infected” links. By doing so, we “isolate” infections, here the spread of supply chain failure. Thus, we minimize inherited failure susceptibility, and increase resilience and minimize network SOC.

Long Links: Better or Worse?

Longer links could be good if we are trying to minimize cascading failures brought on by epidemics, or in the case of CIKR protection, failures brought on by exploiting maritime ports to transship a WMD in a container. However, longer links can also be a burden and increase SOC of CIKR networks. This can be demonstrated with a study of the evolution of the power sector. Over time, this sector has evolved and approached SOC through a combination of economic and regulatory forces. Essentially, longer transmission lines between generation stations and customers have increased the fragility of the power network, as these lines become subject to failure from excessive load.⁵³ The longer links have the opposite effect if we are trying to protect our CIKR from failure; instead of making it more difficult for failures to propagate throughout a system, the links themselves are subject to failure. Link density and length may represent a catch 22 for network protection and resilience.

Exceedence Probability

Another concept to consider in resilience analysis is that of exceedence probability. The components of the standard DHS risk equation leverage probabilistic risk analysis (PRA) terms that focus on the probability an attack will be successful given it is attempted. When multiplied by consequence of that attack, we get risk. However, what if we instead consider the probability that the magnitude (consequence) of an event will exceed a certain threshold, rather than focusing on the probability the event will occur in the first place?

This might constitute a paradigm shift of a different flavor. OR advocates have warned against static quantifications of threat, claiming that it fails to account for adaptive adversaries. One shift in response to that concern has been to modify the treatment of threat, through deterrence measurement as described earlier. However, a second shift could be to consider the probability of the consequence exceeding a pre-determined level, hence the term

exceedence probability. This way, the issue with static vs dynamic probabilities of attack occurrence may be bypassed.

The insurance industry uses exceedence probability to set premiums. For examples, see Grossi and Kunreuther.⁵⁴ More recently, Lewis et al. (2011) have used it to classify various hazards CIKR networks face as low risk (high resilience) or high risk (low resilience).⁵⁵ Exceedence probability is used to create a “resilience exponent” of a network, shown in Equation 3:

$$PML = EP(C) = C^{1-q}$$

Equation 3. Probable maximum loss (PML) as a function of resilience exponent “q”⁵⁶

Now, instead of PRA, we have PML as an alternative expression of risk, for systems of CIKR.⁵⁷ q is the resilience exponent, derived from plotting exceedence probability of the system failure exceeding a certain threshold, which yields a power law. If q>1, the system is low risk, or high resilience. If q <1, the system is high risk, or low resilience.

Low risk systems, as characterized by Equation 3, may adapt. High risk systems may collapse and fail, becoming extinct. This distinction between higher and lower-risk systems can be reflected in a feedback loop diagram of “punctuated reality”.

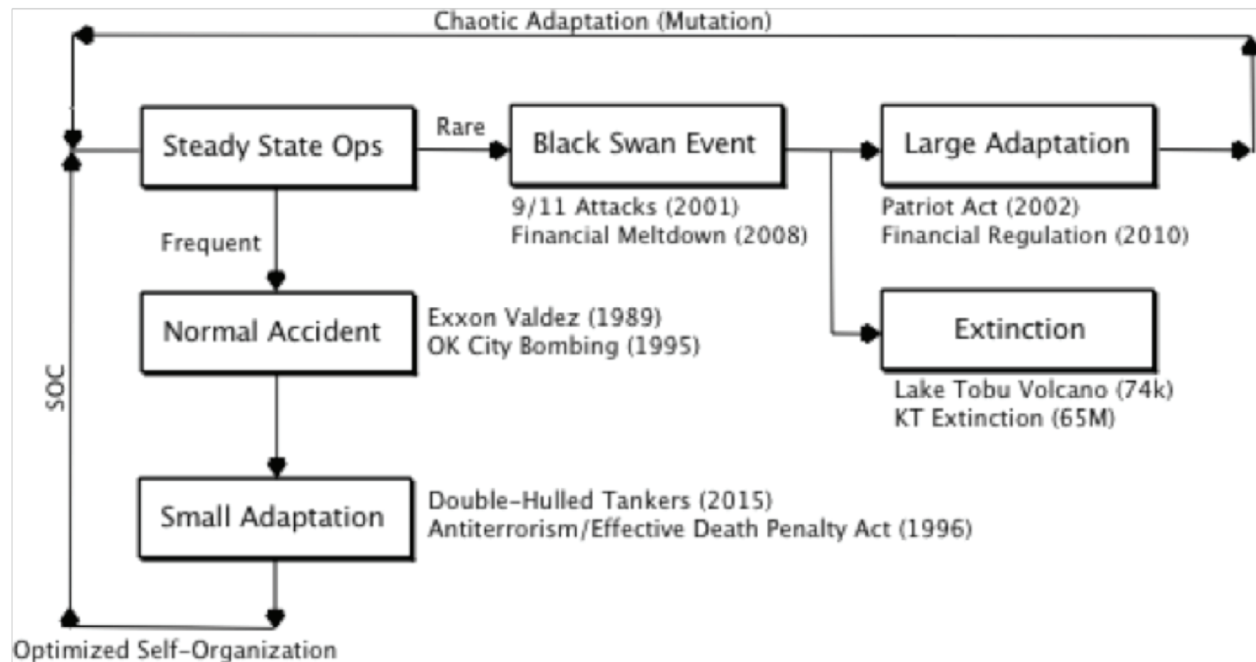


Figure 5. The two major feedback loops of Punctuated Reality⁵⁸

In this depiction, systems evolve and approach SOC. A “normal accident”, punctuating the equilibrium that existed until that point, will occur and the system may adapt, increasing SOC even more and re-establishing a new equilibrium. However, a “black swan” event of much higher consequence but lower probability may occur, driving the system toward extinction rather than adaptation. Low risk (high resilience) systems may be grouped with those that

can achieve small adaptations, but also withstand black swan events, whereas high risk (low resilience) systems may become extinct after a black swan event cripples that system.

Returning to the discussion of supply chain networks and resilience, over time these systems might evolve to become more efficient. However, what happens when a Deepwater Horizon occurs? Arguably this was a Black Swan-type event. This paper does not explore the details of how the petrochemical supply chain in the Gulf of Mexico was impacted, but imagine if the system was optimized such that the Deepwater Horizon platform was the sole source of feedstock to the major Gulf refineries? From an economic standpoint, that might have made sense, but from a redundancy and resilience standpoint, the consequences could be catastrophic.

SOC can be reduced, and system resilience thus increased, by “increasing the resilience exponent” of a system per Equation 3. How do we do this for CIKR systems? Lewis proposes some ways: adding surge capacity, operating systems below capacity, and redesigning networks altogether.⁵⁹ But, these solutions are not without costs.

The Future – “Antifragility”?

In addition to SOC and exceedence probability, can we extend past resilience and apply the concept of antifragility to CIKR protection? Nassim Nicholas Taleb has written about the concept of “antifragility”, which essentially describes systems that actually benefit from disorder, rather than suffer.⁶⁰ He emphasizes in his works that antifragility is not the same as resilience. The latter term means the ability to return to a pre-perturbation state; whereas the former term means the system will exceed pre-perturbation performance levels.

This is an interesting concept to explain complex systems like the stock market, where Taleb has experience and observed phenomena that influenced his theories and publications, but what are the implications, if any, for CIKR system protection and resilience? Taleb differentiates between “mechanical” systems, that wear from use, and “organic” systems, which actually benefit from stress and (reasonable) perturbations.⁶¹ For example, humans as organic “networks” of organ systems and sub-systems benefit from strenuous exercise over time, whereas a washing machine will wear over time with strenuous use, even with consistent maintenance. If we believe CIKR networks are “mechanical” systems, it may be futile to hope perturbations are beneficial. However, if we believe the “organic” model can be applied to CIKR networks, perhaps systems of CIKR can improve after shocks.

For example, how will the Gulf coast petrochemical industry network adapt to Deepwater Horizon? It may be too early to tell, but many years from now, we might compare productivity and other appropriate metrics to pre-Deepwater levels, and conjecture whether this disaster contributed to long term improvement in petrochemical supply chain network management.

An example from popular culture could further illustrate. In *Forrest Gump*, the protagonist’s shrimping vessel was subject to perturbations during the storm, but was robust to the elements and survived, while the rest of the fleet was brittle as they were tied up at the pier and were destroyed by the elements. Gump’s subsequent monopoly on the shrimping industry may reflect a flavor of “antifragility” if we consider the entire shrimping community as a network. In fact, the shrimping business might have improved from pre-storm levels. With less competition, the risk of overexploiting the resource may have diminished, allowing

better stock health and improving the overall market. This may be an example of a mitigating effect on the “tragedy of the commons”, where a common resource is overexploited to the eventual detriment of all. Taleb claims that “the antifragility of some comes necessarily at the expense of others.”⁶²

Organic systems supposedly respond to acute stressors better than chronic stressors.⁶³ As a real world example, one author has claimed downtown Manhattan, as an “economic system”, may have benefitted from the tragedy of 9/11.⁶⁴ It may seem distasteful to claim that long term benefit is a product of disaster, but if we look at the hard numbers, we may have a case. Arguably, 9/11 was an “acute stressor.”

Also, organic networks tend to be self-healing.⁶⁵ During 2012, the New England and New York petrochemical facilities adapted in the aftermath of Hurricane SANDY. They found feedstock from other sources and shared information that they might otherwise manage as proprietary information, to facilitate recovery. Does any data support that those networks are stronger now than they were before SANDY?

Returning to the concept of resilience exponent, the Taleb arguments might extend the utility of this exponent beyond only representing a proxy for system resilience. Could we hypothesize that q could predict antifragility of CIKR networks? The lower the exponent, the more likely the system could benefit from perturbation, increasing output or other performance metrics. This claim would be subject to modeling/simulation and real world event validation.

In our 2013 paper on PSGP resilience, we emphasized that the “desired” post-perturbation system performance level would have to be agreed upon in order to establish a baseline for the resilience modeling effort.⁶⁶ If stakeholders agree that a goal should be to come back stronger after a perturbation, this would transition the notional model from resilience evaluation to antifragility evaluation. It is unclear how specific resilience investments to rebuild damaged infrastructure would increase productivity beyond pre-perturbation levels, but this is an exercise for future research.

However, there are also arguments *against* conceptualizing CIKR networks as organic systems. We might claim that if individual CIKR within a network were antifragile, that means the system is also antifragile. For example, as we improve ability to restore node productivity past pre-perturbation levels, thus improving overall system resilience, we might improve system antifragility. However, Taleb’s claim regarding organic system antifragility is that the individual component is fragile whereas the whole is antifragile. Taleb offers the example of genes: humans are individually fragile and thus die, but we may propagate our genetic information before death, meaning the human race writ large is antifragile.⁶⁷ Therefore, this concept might not apply to networks if we claim improving hubs improves the overall network.

Survival of the Fittest?

Taleb discusses the concept of autophagy, wherein weaker cells in an organism are killed, but the remaining cells become even stronger.⁶⁸ Can we apply this concept to the CIKR network discussion? This might suggest that laissez-faire economic policies to let industry grow unchecked and let market forces govern would be the ideal approach. The weaker

industries would fail or be subject to merger/acquisition. Taleb advocates against excessive intervention in the markets, citing the concept of “iatrogenics” — intervention to manage complex systems that yield long term deleterious effects exceeding benefits of that intervention.⁶⁹

However, Lewis might argue that laissez-faire policies would enable the evolution of SOC in CIKR networks — economic efficiency at expense of resilience. History has shown that various sectors in the economy tend toward SOC when de-regulated. This would make networks fragile, not antifragile. Therefore, some government regulation might be necessary to ensure antifragility.

A third view could be that is it better for overall antifragility to let SOC evolve and then weaker CIKR systems are eliminated during a punctuated equilibrium or Black Swan event. This would be some low probability but extremely high consequence disaster that affected business networks in a way that the SOC made them vulnerable to. The weak networks would collapse; the resilient networks would survive; antifragile systems would “thrive” and benefit from perturbations. Survival of fittest at the “national economy” ecosystem level, if not at the individual CIKR system level, could be the best approach. Managing public expectation for supply of certain commodities would be critical.

Taleb claims “antifragility of higher levels may require the fragility of lower levels within an ecosystem.”⁷⁰ In other words, local but not global overconfidence is good within the economic ecosystem — we want individuals to take risks and fail which means systems should improve over time.⁷¹ We might extend this argument to claim that individual business systems will take risks and fail, which means the *national economy* should in theory improve over time as lessons are learned (and hopefully heeded!)

A final thought on Taleb’s analysis. He discusses “transferring fragility from the collective to the unfit.”⁷² For example, in 2009 the federal government bailed out failing banks. Did this make them more fragile over the long term because they did not have to bear the consequences of their decisions? Applying this logic to the PSGP program, if we subsidize maritime CIKR “hubs” through port security grants, we harden the hubs and increase resilience from a network science perspective — but are we inadvertently harming the system by decreasing self-reliance in those hubs? If left to their own devices but encouraged to be individually antifragile, without government subsidy, would they ignore that encouragement and continue to optimize for economic efficiency but decrease system resilience?

SOC arguably reflects the reverse argument: transfer of fragility from the individually unfit MCIKR to the collective. As a hub accumulates more influence over a network (e.g., through link accumulation) but fails to increase security or individual node resilience, the entire network resilience may suffer as a perturbation to that node could have cascading effects throughout the entire system. Again, we are back to a dilemma: do we allow market forces and deregulation to permit SOC and transfer of fragility from the unfit to the collective, knowing that if a system fails, the next system may or may not be stronger? Or, do we transfer fragility from the collective to the unfit and regulate industry such that resilience is increased but economic efficiency may be stifled? Is there a balance between the two goals?

Alternative Futures

The Lexicon defines “alternative futures analysis” as:

“a set of techniques used to explore different future states developed by varying a set of key trends, drivers, and/or conditions.”⁷³

One example is a statistical forecasting technique known as Winter’s method, used in the past by DHS to project anticipated migrant flow in the Caribbean based on political and economic “push-pull” factors. If these alternative futures techniques included forecasting of probabilities, Taleb might object, as the “black swan” or low probability, high-consequence event cannot be predicted by ordinary probability estimates. Therefore, to have credibility in Taleb’s world, alternative futures analysis might predict the range of possible consequences of an outcome, and then decision makers could hedge for the worst case consequence, rather than relying solely on probability estimates. If we adopted this philosophy, we would be well advised to look at the magnitude and reach of previous disasters, and optimize systems for these consequences first, and then make refinements for economic efficiency second.

Putting It All Together: Implications for CIKR Protection and Resilience?

We have given examples of how to analyze threat, vulnerability, and consequence in different ways. If we use intent as the output of game theoretic modeling, our risk equations may account for “tactical intelligence” as well as “strategic intelligence” and may have implications for deterrence. If we model layered defenses against terrorist transfer of WMD as a network and use logic gates as proxies for attacker preferences, absent more specific intelligence, this approach may provide us with alternate analysis to inform where to invest in WMD detection technology. If we model ports as “hubs” with downstream customer networks, and estimate network resilience, that may have implications for how we allocate funding to protect our port infrastructure through grant programs.

Also, if we calculate exceedence probability and probable maximum loss to CIKR networks instead of the traditional PRA calculations, would this have implications for how we allocate resources? Should we allocate prevention-based resources to high risk/low resilience systems to try and protect against the “black swans”? For higher-resilience or lower risk systems, should we allocate resources toward responding to higher probability, but lower consequence events? Finally, is resilience enough? Are there ways to engineer CIKR systems to come back even stronger after a perturbation, or promote “antifragility”?

The Lexicon defines “risk governance” as:

“actors, rules, practices, processes, and mechanisms concerned with how risk is analyzed, managed, and communicated.”⁷⁴

If we believe the theories behind CIKR risk analysis, protection, and resilience are evolving, then that naturally influences the “rules, practices, and processes” concerned with how risk is analyzed, managed, and communicated. The DHS Quadrennial Homeland Security Review (QHSR) of 2014 emphasizes deterring terrorists, interdicting WMDs, and safeguarding legal trade.⁷⁵ It also acknowledges CIKR network interdependencies, and that networked partnership is important to combat terrorism. We hope that the ideas posed in this paper will help inform theory and practice as the homeland security and emergency management enterprise evolves in its understanding of risk.

About the Authors

Eric F. Taquechel is a U.S. Coast Guard officer with experience in shipboard operations, port operations, critical infrastructure risk analysis, contingency planning/force readiness, operations analysis, budget/personnel management, and planning, programming, budgeting, and execution processes. He has authored and coauthored various publications including “Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction,” in *IEEE Network Magazine*; “How to Quantify Deterrence and Reduce Critical Infrastructure Risk,” in *Homeland Security Affairs Journal*; “Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program,” in the *Journal of Homeland Security and Emergency Management*; “Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent Risk Reduction,” in *Homeland Security Affairs Journal*, and most recently, “More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases”, in *Homeland Security Affairs Journal*. Taquechel has taught college courses on critical infrastructure protection and is a FEMA Master Exercise Practitioner. He earned a master’s degree in Security Studies from the Naval Postgraduate School and prior to that earned his undergraduate degree at the U.S. Coast Guard Academy, and is currently an MPA candidate at Old Dominion University. Taquechel (corresponding author) may be contacted at etaqu001@odu.edu.

Ted G. Lewis is an author, speaker, and consultant with expertise in applied complexity theory, homeland security, infrastructure systems, and early-stage startup strategies. He has served in government, industry, and academe over a long career, including Executive Director and Professor of Computer Science, Center for Homeland Defense and Security, Naval Postgraduate School; Senior Vice President of Eastman Kodak; President and CEO of DaimlerChrysler Research and Technology, North America, Inc.; and Professor of Computer Science at Oregon State University, Corvallis, OR. In addition, he has served as the Editor-in-Chief of a number of periodicals: *IEEE Computer Magazine*, *IEEE Software Magazine*, as a member of the IEEE Computer Society Board of Governors, and is currently Advisory Board Member of *ACM Ubiquity and Cosmos+Taxis Journal* (The Sociology of Hayek). He has published more than 35 books, most recently including *Book of Extremes: The Complexity of Everyday Things*, *Bak’s Sand Pile: Strategies for a Catastrophic World*, *Network Science: Theory and Applications*, and *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Lewis has authored or co-authored numerous scholarly articles in cross-disciplinary journals such as *Cognitive Systems Research*, *Homeland Security Affairs Journal*, *Journal of Risk Finance*, *Journal of Information Warfare*, and *IEEE Parallel & Distributed Technology*. Lewis resides with his wife, in Monterey, California.

Acknowledgements

In addition to all the anonymous (and occasionally non-anonymous) referees who helped improve the quality of the work previously published, the authors wish to thank the Center for Homeland Defense and Security, in particular the University-Agency Partnership Initiative, for the invitation to present a summary of this work at the 10th Annual Homeland Defense/ Security Education Summit in March 2017.

Disclaimer

The original opinions and recommendations in this work are those of the authors and are not intended to reflect the positions or policies of any government agency.

Notes

- 1 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), <https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>, Web accessed February 18, 2017.
- 2 Ibid.
- 3 Ibid.
- 4 Louis A. Cox, "Some Limitations of 'Risk=Threat x Vulnerability x Consequence' for Risk Analysis of Terrorist Attacks," *Risk Analysis* 28(2008): 1749-1761.
- 5 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 6 Zhengyu Yin et al., "Stackelberg vs. Nash in Security Games: Interchangeability, Equivalence, and Uniqueness", *Proceedings of the Ninth International Conference on Autonomous Agents and Multiagent Systems*, (2010), <http://teamcore.usc.edu/papers/2010/AAMAS10-OBS.pdf>, Web accessed February 18, 2017.
- 7 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 8 Ibid.
- 9 Ibid.
- 10 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: Wiley Interscience, 2006).
- 11 Ted G. Lewis, *Network Science: Theory and Applications* (Hoboken, NJ: Wiley Interscience, 2009).
- 12 Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World* (Williams, CA: Agile Press, 2011).
- 13 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 14 Eric D. Vugrin et al., "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, eds. Kasthurirangan Gopalakrishnan and Srinivas Peeta (New York: Springer, 2010), 77-116.
- 15 <https://www.dhs.gov/topic/resilience>.
- 16 Eric F. Tauechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8(August 2012), <https://www.hsaj.org/articles/226>, Web accessed February 18, 2017.
- 17 Ibid.
- 18 Eric F. Tauechel, "Validation of Rational Deterrence Theory: Analysis of U.S. Government and Adversary Risk Propensity and Relative Emphasis on Gain or Loss," Master's Thesis, Center for Homeland Defense and Security (2010), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA519012, Web accessed February 18, 2017.
- 19 Waleed I. Al Mannai and Ted. G. Lewis, "A General Defender-Attacker Risk Model for Networks," *Journal of Risk Finance* 9 (2008): 244-261.
- 20 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 21 Ibid.
- 22 Ibid.
- 23 Ibid.
- 24 Ibid.

- 25 Amos Tversky and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science* 217(1981): 453-584.
- 26 Daniel Kahneman, *Thinking Fast and Slow*, (New York: Farrar, Straus, and Giroux, 2011).
- 27 Eric F. Tauechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs* 12(September 2016), <https://www.hsaj.org/articles/12007>, Web accessed February 18, 2017.
- 28 Daniel Moran, "Strategic insight: Deterrence and Preemption," *Strategic Insights* 1(2008), <https://www.hsd.org/?view&did=1428>, Web accessed February 18, 2017.
- 29 Kevin Chilton and Greg Weaver, "Waging Deterrence in the Twenty-First Century," *Strategic Studies Quarterly* (2009): 31-42. <http://www.au.af.mil/au/ssq/2009/Spring/chilton.pdf>, Web accessed February 18, 2017.
- 30 Eric F. Tauechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk."
- 31 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 32 Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*.
- 33 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 34 Eric F. Tauechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction," *IEEE Magazine* 24(2010): 30-35
- 35 Ted G. Lewis, *Network Science: Theory and Applications*.
- 36 Ibid.
- 37 Eric F. Tauechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction."
- 38 Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World*.
- 39 Ibid.
- 40 Eric F. Tauechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs* 11(February 2015), <https://www.hsaj.org/articles/1304>, Web accessed February 18, 2017.
- 41 Ibid.
- 42 The White House, *Maritime Commerce Security Plan for the National Strategy for Maritime Security*, (2005), https://www.dhs.gov/xlibrary/assets/HSPD_MCSPPlan.pdf, Web accessed February 18, 2017.
- 43 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 44 Ibid.
- 45 Eric F. Tauechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management* 10(2013): 521-554.
- 46 U. S. Department of Homeland Security, *DHS Risk Lexicon*
- 47 Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World*.
- 48 Ibid.
- 49 Ted G. Lewis, *Network Science: Theory and Applications*.
- 50 Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World*.

- 51 Ibid.
- 52 Ibid.
- 53 Ibid.
- 54 Patricia Grossi and Harold Kunreuther, *Catastrophe Modeling: A New Approach to Managing Risk* (New York: Springer, 2005).
- 55 Ted G. Lewis, Tom Mackin, and Rudy Darken, "Critical Infrastructure as Complex Emergent Systems," *International Journal of Cyber Warfare and Terrorism* 1(2011): 1-12.
- 56 Ibid.
- 57 Ibid.
- 58 Ted G. Lewis, *Bak's Sand Pile: Strategies for a Catastrophic World*.
- 59 Ibid.
- 60 Nassim Nicholas Taleb, *Antifragility: Things that Gain from Disorder* (New York: Random House, 2011).
- 61 Ibid.
- 62 Ibid.
- 63 Ibid.
- 64 David Riedman, "Questioning the Criticality of Critical Infrastructure: A Case Study Analysis," *Homeland Security Affairs* 12(May 2016), <https://www.hsd.org/?view&did=793055>, Web accessed February 18, 2017.
- 65 Nassim Nicholas Taleb, *Antifragility: Things that Gain from Disorder*.
- 66 Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program".
- 67 Nassim Nicholas Taleb, *Antifragility: Things that Gain from Disorder*.
- 68 Ibid.
- 69 Ibid.
- 70 Ibid.
- 71 Ibid.
- 72 Ibid.
- 73 U. S. Department of Homeland Security, *DHS Risk Lexicon*.
- 74 Ibid.
- 75 U. S. Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review* (2014), <https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>, Web accessed February 18, 2017.

Copyright © 2017 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).



The Roots of Community Resilience: A Comparative Analysis of Structural Change in Four Gulf Coast Hurricane Response Networks

By Thomas W. Haase, Gunes Ertan, and Louise K. Comfort

Abstract

Despite the emphasis on resilience, disasters continue to challenge the response capacities of communities around the United States. These challenges are generated by the complexities and uncertainties present in the post-disaster environment. This article presents the findings of an exploratory investigation into the development and evolution of four disaster response networks that formed along the Gulf Coast, Hurricane Katrina and Hurricane Rita in 2005, and Hurricane Gustav and Hurricane Ike in 2008. Using data collected from newspaper articles that referenced each hurricane during a period that spanned six days prior to landfall to twenty-two days after landfall, we identified the organizations that participated in each response network. We then used UCINET 6 to calculate network density and degree centralization, plotted longitudinally by date, and evaluated whether each network underwent structural change. The findings demonstrate that all four response networks underwent structural change, as a large heterogeneous collection of response organizations came together, collected and disseminated information, and sought to identify and implement solutions that would address the needs of those affected by the disaster event. While additional research is necessary to reveal the causal factors behind these structural changes, the findings presented in this article suggest that investments in information communication technologies, such as those made by the state of Louisiana after Hurricane Katrina, can help to facilitate the resilience of disaster response networks.

Suggested Citation

Haase, Thomas W., Gunes Ertan, and Louise K. Comfort. "The Roots of Community Resilience: A Comparative Analysis of Structural Change in Four Gulf Coast Hurricane Response Networks." *Homeland Security Affairs* 13, Article 9 (October 2017). <https://www.hsaj.org/articles/14095>

Introduction

The concept of resilience has become a central focus of emphasis for disaster and emergency management researchers and policy-makers. The United States Department of State officially recognized resilience, defined as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."¹ The U.S. National Academy of Sciences (2012) further refined this definition in its report, *Disaster Resilience: A National Imperative*, which serves as a working guide to resilience studies in both research and practice. Likewise, the Department of Homeland Security indicated that strengthening resilience was one of its five critical missions in its *2014 Quadrennial Homeland Security Review*.² The Federal Emergency Management Agency (FEMA) also considers resilience to be a component of its *National Preparedness Goal*, which it identifies as "[a] secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."³

Despite the emphasis on resilience as a public policy goal, disasters continue to challenge the response capacities of communities around the United States. These challenges are generated by the complexities and uncertainties present in the post-disaster environment.

For public managers, complexity refers to the characteristics of a system, which means that complexity can refer to ill-structured administrative problems,⁴ mismatches between organizational structures and operational conditions,⁵ and the inability to identify and understand the linkages that exist within a system.⁶ Uncertainty, in contrast, refers to the sense of doubt that blocks or delays a decision maker's actions.⁷ According to Elinor Ostrom, policy institutions often provide policy actors with the opportunity to pursue multiple policy choices.⁸ Since the choices taken by policy actors are often interdependent, this variety of choices can create uncertainty in the policy environment. Thus, a decision maker may know the type of action that she should take to obtain a certain outcome, but in an uncertain environment, she is unable to predict with any degree of confidence which of the possible actions will enable her to obtain the desired outcome.

In a disaster management context, complexities and uncertainties can undermine administrative effectiveness⁹ and generate cascades of failures.¹⁰ When such failures occur, the activities undertaken by disaster response organizations can become delayed, sporadic and ineffective, thereby leaving vulnerable populations subject to further risk. Recognizing this constraint, some governments have sought to manage uncertainty and complexity by using information technologies to facilitate information exchange and improve decision making.¹¹ Thus, an important question is whether, and to what extent, access to information shapes the capacity of an organizational network to mobilize and structure disaster response operations?

This article presents the findings of an exploratory investigation into whether investments in information technology can affect the structural development and evolution of four disaster operations networks that formed in response to hurricanes along the Gulf Coast.¹² Two of these networks formed in 2005 after Hurricane Katrina in Louisiana and Hurricane Rita in Texas. The other two networks formed in 2008 after Hurricane Gustav in Louisiana and after Hurricane Ike in Texas. After a brief introduction to resilience, this article explores three streams of literature relevant to this inquiry: inter-organizational network theory, complex adaptive systems theory, and social-technical systems theory. The second section reviews the four cases investigated by this study, focusing on the consequences of the events and the operational conditions under which the disaster response networks emerged. The third section presents the study's research questions and methods of analysis. After the presentation of the findings, the article concludes by identifying policy implications for improving resilience of disaster response networks.

Resilience as an Evolving Concept

Aaron Wildavsky defined resilience as "the capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back."¹³ Alternative definitions construe resilience as the adaptability of systems to new environments through rapid transformation of existing resources to new demands. These approaches underline the role of information and information exchange in the facilitation of resilience.¹⁴ Although the focus of significant discussion, disaster management scholars and practitioners have yet to formulate a consensus as to what resilience means and how resilience should be evaluated. Recent research into the components and indicators of community resilience, however, has begun to advance the study of resilience.¹⁵ Ashley Ross, for example, conceptualizes resilience as a dynamic phenomenon that is driven by a set of adaptive capacities and processes.¹⁶ In this article, we applied this definition of resilience to the study of disaster response networks.

Three streams of literature are relevant to this investigation of resilience in disaster response networks.

Inter-Organizational Networks

According to Michael McGuire, networks are “multiorganizational arrangements for solving problems that cannot be achieved, or achieved easily, by a single organization.”¹⁷ These networked arrangements are considered superior to traditional administrative structures. Networks provide an alternative to hierarchy and specialization, meaning they can accommodate a diversity of organizations – public, private, and nonprofit – which can work together to achieve collective goals.¹⁸ Networks are also highly flexible, enabling their constituent organizations to adapt their interactions in response to changes in the operational environment. Further, networks are scalable to the extent that their participants have the capacity to seek assistance from other organizations, whether vertically by level of jurisdiction or horizontally by source of funding. Finally, networks enable participants to identify and acquire the information and resources they need to complete their activities.¹⁹

Provan and Kenis note that networks provide a community of organizations with the structure they need to interact with one another and engage in learning activities.²⁰ As such, a network of organizations designs a structure that enables its members to learn how to modify their activities within, and in response to, the complexities and uncertainties present in the operational environment.²¹ Similarly, a network’s interaction structure can facilitate the efficient distribution of resources, which is important for disaster response networks.²² As they work to structure and re-structure their relationships, organizations in a disaster response network can quickly locate resources such as information, money, personnel and equipment, and move these resources to where they are needed. Although the inter-organizational network literature suggests that networked governance structures are better positioned than traditional governmental structures to address the dynamic and ill-structured policy problems, the literature does not specify the processes that organizations would use to overcome the uncertainties and complexities present in the operational environment.

Proposition 1: A resilient disaster response network will be comprised of a heterogeneous collection of organizations that interact with one another to pursue and obtain collective goals.

Complex Adaptive Systems

A second stream of literature suggests that a disaster response network comprised of a heterogeneous collection of organizations may have the capacity to adapt in response to the uncertainties and complexities of changing environments.²³ This adaptive capacity emerges when a system of organizations operates as a complex adaptive system, that is, a non-linear system of interdependent agents that collectively learn how to adjust their activities in reaction to environmental changes.²⁴ The agents present in such systems receive information about the external environment. When a decision is needed, agents use internal models of rules to analyze the information they receive, which gives them insight into the actions that they should take. These rules draw upon internal cognitive building blocks, which agents employ to simplify their environment.²⁵ In the public administration context, these building blocks take the form of signals that may be communicated through

memoranda and directives, and boundaries that may be established by legislation and agency mission statements.²⁶

Complex adaptive systems theory can be used to investigate the resilience of disaster response networks. In the words of Robert Axelrod and Michael Cohen, a system of agents can harness complexity by acknowledging the interdependent relationships that exist in a system and taking deliberate action to restructure the system to align with a desired measure of performance.²⁷ For example, a policy-maker might encourage the organizations in a disaster response network to modify their actions by permitting them to exploit emergent opportunities and rewarding them when they identify novel solutions.²⁸ Policy-makers may encourage organizations to modify their interaction patterns by enabling them to make internal procedural adjustments or by adjusting their operational environment, perhaps by exempting them from regulatory requirements during a crisis. Finally, policy-makers may encourage organizations to identify and select successful strategies by providing them with a clear understanding of what constitutes success, and rewarding them when they cast aside ineffective strategies.²⁹ In a disaster context, inter-organizational relationships are a central aspect of this adaptive process because they lead to the development of “networks of reciprocal interaction that foster trust and cooperation.”³⁰

Proposition 2: Learning, adaptation, and structural adjustment to environmental uncertainties and complexities are indicators of resilience in a disaster response network.

Sociotechnical Systems and Information Technology

A third stream of literature suggests that information technology can support a disaster response network's capacity to adapt to uncertainty and complexity. That is, information technology represents a tool that can bring together a disconnected and spatially separated community of organizations.³¹ Information technology provides officials with the ability to scan the operational environment, detect and verify potential risks, and transmit risk and response information across an expansive network of organizations charged with disaster management and operational responsibilities.³²

Albert Charns argued that the integration of technology within a social structure leads to the development of a sociotechnical system.³³ Herbert Simon considered design as a means of structuring relationships among human beings, organizations, and technology.³⁴ A sociotechnical system drives the processes of adaptation within a networked system, thereby enabling it to adjust and reorganize as required by changing conditions in the environment.³⁵ There are several ways that technology can strengthen the capacities for performance and processes of adaptation in disaster response networks. The National Academies of Sciences identified three disaster management functions that were enabled through information technology: 1) robust, interoperable and priority-sensitive communications; 2) development of situational awareness and common operating picture; and 3) improved decision support, resource tracking, and resources allocation.³⁶ All three functions are supported by information technology that, properly designed and implemented, can facilitate learning and adaption in a disaster response network.

Proposition 3: Information Communication Technologies (ICT), properly designed and implemented, can facilitate resilience (learning, adaptation, and structural adjustment) within disaster response networks.

An extensive body of literature focuses on networks and their roles in disaster management contexts. Empirical investigations of disaster response networks, for example, often focus on networks at a specific point in time (e.g., a single day) or as an aggregation of several points in time (e.g., a collective set of days or weeks). Investigations such as these have demonstrated the importance of disaster response networks and the existence of problematic resource and information gaps between organizations.³⁷ In the context of resilience, however, these studies provide little insight into how disaster response networks emerge or evolve over time. Further, the literature on disaster response networks says little about network effectiveness, suggesting that the factors or conditions that promote or inhibit the resilience of disaster response networks are not yet fully identified. Relatedly, the extent to which policy changes might influence the emergence, evolution, and performance of disaster response networks is not yet known.

Case Study Selection

To evaluate the three propositions identified above, we conducted a small-n case study of the interaction structures of disaster response networks that formed after four Gulf Coast hurricanes. Specifically, we identify and compare the structural features of the organizational response networks that formed in 2005 following Hurricane Katrina in Louisiana and Hurricane Rita in Texas, with those that formed in 2008 following Hurricane Gustav in Louisiana and Hurricane Ike in Texas.

Louisiana: Hurricane Katrina, 2005 and Hurricane Gustav, 2008

Classified as one of the deadliest disaster events in the history of the United States, Hurricane Katrina struck the coast of Louisiana east of New Orleans the morning of August 29, 2005. Although New Orleans managed to withstand Hurricane Katrina's impact, the storm surge and rainfall-induced flooding caused the subsequent failure of the levee systems, which inundated large portions of the city. In the days that followed, disaster management officials worked to avert an even larger humanitarian catastrophe. The federal government reported that Hurricane Katrina affected 41 of the state's 64 parishes, caused approximately 1,100 deaths, and generated US\$ 100 billion of damage.³⁸ Approximately three years later, on September 1, 2008, Hurricane Gustav came ashore in Terrebonne Parish, Louisiana as a Category 2 storm. The National Weather Service reported that Hurricane Gustav weakened to a tropical depression, but continued to produce severe winds, tornados, and substantial rainfall, as much as twenty-one inches in some areas, as the storm slowly moved north beyond Baton Rouge.³⁹ In Louisiana, Hurricane Gustav was responsible for seven deaths and an estimated US\$ 4.618 billion of damages.

Texas: Hurricane Rita, 2005 and Hurricane Ike, 2008

Less than three weeks after Hurricane Katrina, a Category 5 Hurricane called Rita was moving towards the western coast of the Gulf of Mexico.⁴⁰ Given the devastation wrought by Hurricane Katrina, government officials were concerned about the threats that Hurricane Rita posed to the oil and gas industry. Equally important, Hurricane Rita threatened the city

of Houston, so officials ordered wide scale evacuations. According to the National Weather Service, Hurricane Rita came ashore between Sabine Pass, Texas and Johnson's Bayou the morning of September 24, 2005 as a Category 2 Hurricane. Fortunately, the region avoided a catastrophe, with only two reported fatalities. Nevertheless, Hurricane Rita caused more than US\$ 12 billion of damages. In after action reports, discussions about the governmental response to Hurricane Rita focused on the massive traffic jams caused by the evacuation orders. On September 13, 2008, almost three years after Hurricane Rita, a Category 2 storm named Hurricane Ike made landfall near Galveston, Texas.⁴¹ Along Galveston Bay, the storm surge increased to between ten and fifteen feet. Hurricane Ike's sustained winds generated several tornados and severely damaged Houston's downtown area. The storm took the lives of 21 Texans, and at least 16 people remained missing as of August 2011. Hurricane Ike became the third most expensive hurricane in the history of the United States, with damages estimated to be more than US\$ 29.5 billion.⁴²

Separated by a period of three years, these two sets of hurricane events make it possible to compare the structures of the disaster response networks that emerged to operate in the same general region of the United States. Many of the organizations, especially the public emergency management agencies, were present in both Louisiana and Texas for all four hurricanes, which increases the comparability of these disaster response networks. However, while activities of Texas and Louisiana were guided by federal laws and policies, each state had developed different perceptions of risk, and made different policy choices regarding the management of information in their respective communities in the months and years that followed the first hurricane event. Given that these four cases represent a valid small-n field study for the examination of the resilience of disaster response networks, we investigate the theoretical propositions stated above through an exploration of four comparative research questions:

1. To what extent were the four disaster response networks characterized by heterogeneity in contrast to homogeneity in the respective sets of participating organizations?
2. At what rate did response organizations interact with other organizations in these four disaster response networks?
3. To what extent did the interactions exchanged among response organizations drive the structural evolution of these four disaster response networks?
4. To what extent did investments in information technology and training between hurricane events facilitate structural changes in the disaster response networks?

Methods

This article investigates the resilience of the disaster response networks that emerged after hurricanes that occurred in 2005 and 2008: Hurricanes Katrina and Gustav in Louisiana and Hurricanes Rita and Ike in Texas. To answer the research questions stated above, we collected, coded, and analyzed data obtained from newspaper articles and government reports that covered the response activities that occurred before and after the hurricanes made landfall. The processes that we used to collect and analyze our data are discussed in the following subsections.

Data Collection and Coding

The data came from newspaper articles from the *Times Picayune* and the *Houston Chronicle*, which are respectively published in New Orleans, Louisiana and Houston, Texas. These articles covered the activities undertaken by the response networks that formed after each hurricane event, and constitute a day-to-day record of the activities undertaken by the organizations participating in each network. To focus our data collection activities, we used time and shared behavior to set the boundaries of the disaster response networks.⁴³ Then, we conducted keyword searches in the *LexisNexis Academic Database* to identify articles that referenced each hurricane by name and were published between six days prior to landfall and twenty-two days after the storm made landfall. We classified articles as relevant if they referenced activities that fell within the fifteen Emergency Support Functions (ESFs) covered by the *National Response Plan*⁴⁴ and the *National Response Framework*.⁴⁵

We then coded the content of the newspaper articles and created *Excel* databases for each hurricane response network. To create these databases, we reviewed each article and identified the organizations reported to be involved in the response network. We assigned each organization a numerical identifier and an acronym, and classified the organizations by the date they became active in the response network, their source of funding (public, private, or nonprofit) and their level of jurisdiction (national, regional, state, county, or city). We also identified the interactions exchanged between organizations and coded each interaction as a separate transaction. All interactions were coded as non-directional and unweighted, since the news articles did not always indicate which organization initiated the transaction or the number of interactions that occurred.

We removed duplicate and irrelevant entries from the *Excel* databases and cleaned the data to ensure the consistency in organizational names, acronyms, source of funding, and level of jurisdiction. To ensure reliability, all co-authors participated in the coding processes and we conducted weekly comparisons to corroborate coding results. We also cross-referenced results from the content analysis with activities reported in government situation reports and found them to be consistent. After the databases were finalized, they were converted into four sets of relational matrices. We generated one set for each hurricane event, with each set comprised of twenty-eight separate relational matrices. Each relational matrix represented one day included in the analysis. We then refined each matrix by excluding isolated organizations, meaning we removed organizations that were not engaged in interactions with other organizations.

Data Analysis

We used multiple methods to analyze the data for each of the disaster response networks. We began by generating descriptive statistics to reveal the organizational composition of each network. We used *Excel* to generate tables that reported the numbers, jurisdictional levels, sources of funding and frequency distributions of the organizations detected in each disaster response network. We also plotted longitudinally, by date, the rate that the organizations became active in each disaster response system, as well as the number and type of interactions undertaken by each organization. We used these data to address our first and second research questions.

We used the network analyses software UCINET 6 to evaluate the data contained in our four sets of relational matrices.⁴⁶ We used two common network level network measures to reveal the structure of the networks: density and degree centralization. We calculated these statistics for each of the twenty-four relational matrices included the period under analysis, and plotted the results longitudinally, by date, to evaluate whether each network underwent structural change. We then used these data to address our third research question. To address our final question, we reviewed governmental reports to determine whether Texas and Louisiana underwent policy changes or made investments in information technology between 2005 and 2008.

Research Assumptions

The application of the methods described above were subject to four assumptions, which enabled us to isolate the changes in interaction patterns within response networks that were stable in size across equivalent time slices. First, we assumed that the organizations did not enter a response network, but rather, they were always present in the network and became active when they started to interact with other organizations. Second, we assumed that organizations did not leave the response networks, but rather, they maintained a presence throughout the duration of the period under analysis. In line with these two assumptions, for all of the response networks, we used the total number of organizations detected in a network to normalize the number of nodes contained in each network's daily matrices. Third, we assumed that the appropriate window of analysis for the investigation of structural change was twenty-four hours. This decision was driven by the nature of newspaper reporting, but also because larger time slices would undermine our ability to determine if, and when, structural changes might have occurred. Finally, we assumed that the detection of an interaction between two or more organizations represented the establishment of a permanent relationship that lasted throughout the duration of the disaster response. To capture this representation, we created our daily meta-matrices on a cumulative basis. As such, matrix one represented the interactions detected in day one, matrix two represented the interaction detected in day one and day two, and matrix three represented the interactions detected in day one, day two, and day three. This process continued until the creation of the final matrix, which represented the disaster response network in its entirety.

Findings

The findings indicate that the disaster response networks that operated after four hurricane events, Hurricane Katrina in Louisiana and Hurricane Rita in Texas in 2005 and Hurricane Gustav in Louisiana and Hurricane Ike in Texas in 2008, were comprised of a heterogeneous collection of response organizations. Additionally, these organizations modified their behaviors, at least in terms of their inter-organizational interaction patterns, which may suggest that these networks underwent the adaptive processes needed to overcome the uncertainties and complexities present in the post-disaster environment. However, as the findings presented below indicate, the characteristics of these four response networks were not identical.

System Composition

We began our analysis by generating frequency statistics that revealed the number and nature of the organizations that participated in the four response networks. In terms of numbers of organizational participants in the Louisiana networks, the data indicate that the Katrina response network was larger than the Gustav response network, at 372 and 222 organizations respectively. In Texas, the situation was reversed, with more organizations participating in the Ike response network than in the Rita response network, at 372 and 214 organizations respectively. This result is likely because Hurricane Katrina and Hurricane Ike were the biggest storm events under analysis. Further exploration of the data revealed that each response network depended on contributions of organizations from multiple levels of jurisdiction. Reflecting the idea that all disasters are local, the organizations from jurisdictions classified as county/parish level or lower were the most represented in all four response networks: Katrina (172 or 46.24%); Gustav (117 or 52.70%); Rita (113 or 53.24%); and Ike (235 or 63.17%). The organizations from jurisdictions classified as federal and national, which included both government agencies, nonprofit organizations, and private businesses were the second most represented in the response networks: Katrina (94 or 27.27%); Gustav (52 or 23.42%); Rita (44 or 20.37%); and Ike (84 or 22.58%). This was followed by the organizations from jurisdictions classified as state and regional: Katrina (79 or 21.24%); Gustav (48 or 21.62%); Rita (42 or 19.44%); and Ike (42 or 11.29%).

Table 1. Organizational Composition of Hurricane Response Networks by Source of Funding

	LOUISIANA				TEXAS			
	Katrina		Gustav		Rita		Ike	
	N	%	N	%	N	%	N	%
Nonprofit	61	16.40	42	18.92	36	16.82	98	26.34
Private	77	20.70	41	18.47	29	13.55	55	14.78
Public	234	62.90	139	62.61	149	69.63	219	58.87
Totals	372	100	222	100	214	100	372	100

Analysis of the organizational data by source of funding revealed similar findings. As Table 1 indicates, public organizations played a substantial role in response activities following each disaster event. More specifically, these data indicate that approximately 60% of the organizations detected interacting within all four response networks were public organizations. The other sectors also made important contributions to the response networks, but depending on the state, their participation reported slightly different numbers. Although there were fewer total organizations detected in the Gustav network than in the Katrina network, the Gustav network contained a higher percentage of nonprofit organizations than did the Katrina network, at 18.92% and 16.40% respectively. The opposite occurred in Texas, where both the number and percentage of nonprofit organizations increased from Hurricane Rita to Hurricane Ike. Further, in comparison to the other three hurricanes, more nonprofit organizations reported interacting in the response network that formed after Ike, at 26.34%, than in any other network. These data indicate that all four networks were comprised of a heterogeneous collection of organizations, necessary to promote adaptation in response to complexity and uncertainty.

System Growth and Development

We continued analysis of the response networks by plotting the date that each organization became active, meaning that an organization began to interact with one or more organizations in the network. Figure 1 presents the comparative results for Hurricane Katrina and Hurricane Gustav. These data indicate that both networks experienced steady growth over time.

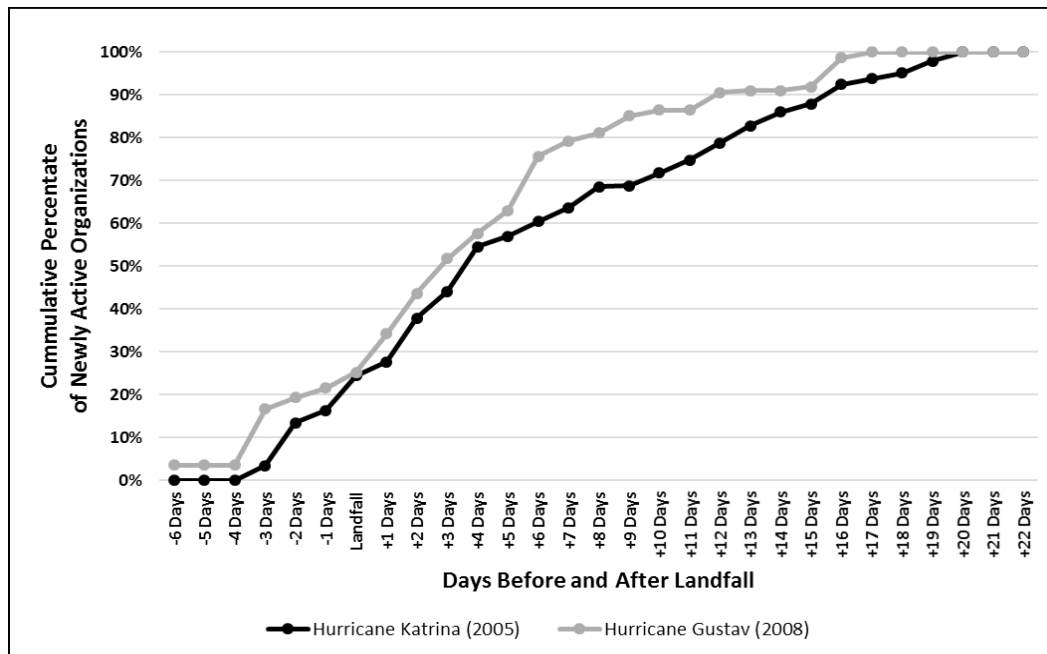


Figure 1. Cumulative Percentage of Newly Active Organizations Detected in Response Network by Day: Hurricane Katrina and Hurricane Gustav

For both the Katrina and Gustav response networks, one quarter of the identified organizations were active by landfall. After landfall, the organizations in the Gustav network, as a percentage of all identified organizations, became active more quickly than the organizations in the Katrina network. By means of comparison, in the Gustav network, 75.7% of organizations were active six days after landfall. At that same time, only 60.5% of the organizations were active in the Katrina network. Subsequently, the organizations in the Gustav network continued to become active at a faster rate, allowing the network to reach 100% capacity sixteen days after landfall. In contrast, the Katrina response network did not reach 100% capacity until twenty days after landfall.

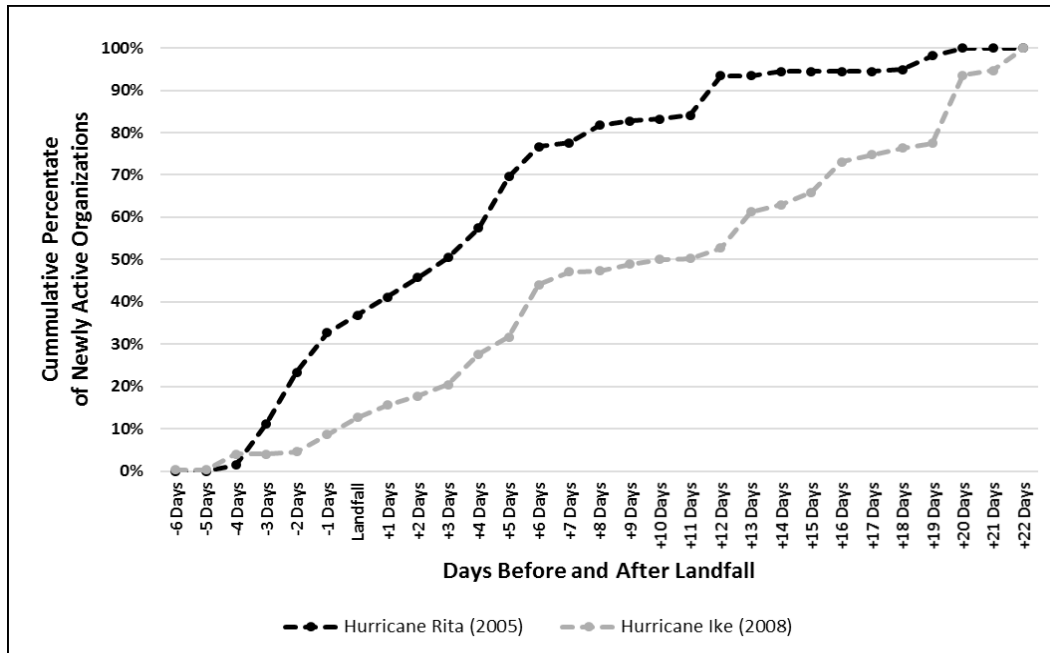


Figure 2. Cumulative Percentage of Newly Active Organizations Identified in Response Network by Day: Hurricane Rita and Hurricane Ike

Figure 2 presents the comparative results for Hurricane Rita and Hurricane Ike. These data indicate that both response networks also experienced steady growth over time. Unlike the Louisiana response networks, however, there were marked differences in the activation rates in the Texas response networks. For example, when Hurricane Rita made landfall, approximately three weeks after Hurricane Katrina, 39.9% of all organizations identified in the Rita network were active. Three years later, when Hurricane Ike made landfall, only 12.6% of the organizations in the response network were active, a substantial drop from the findings for the Rita response network. The expansion of the Ike response network also proceeded at a slower rate, with 61.3% of the identified organizations active thirteen days after landfall, and all identified organizations active in the network nine days later. In contrast, 57.5% of the organizations identified in the Rita response network were active four days after the hurricane came ashore.

System Structural Evolution Over Time

We generated social network measures for the four response networks for each date included in this study. For this article, we investigated two common network measures: density and degree centralization. Wasserman and Faust define network density as the “proportion of the possible [links] that are actually present in a [network].”⁴⁷ In contrast, degree centralization evaluated the extent to which actors have links to each of the other actors in the network. When applied to the network, the degree centrality measure is a quantification of the “range or variability of the individual actor’s indices.”⁴⁸

Network Density

The network density scores for Hurricane Katrina and Hurricane Gustav plotted over time are presented below in Figure 3. These results indicate that the overall density scores for both response networks were low, which is a common feature of large networks. Over time, however, the organizations in both networks became increasingly active. A closer look at the data reveals that the densities of the response networks began to diverge after the hurricanes came ashore. For the Katrina network, the density increased from 0.000884 at landfall to 0.007695 twenty-two days later. In contrast, for the Gustav network, density increased to 0.005585 five days after landfall. Then, on the sixth day, the network's density increased substantially to 0.011088, after which density gradually increased to 0.014879. On the day that this substantial jump in density occurred, FEMA was working with several state and parish organizations to open a major aid center, which began to distribute assistance to communities affected by Hurricane Gustav.

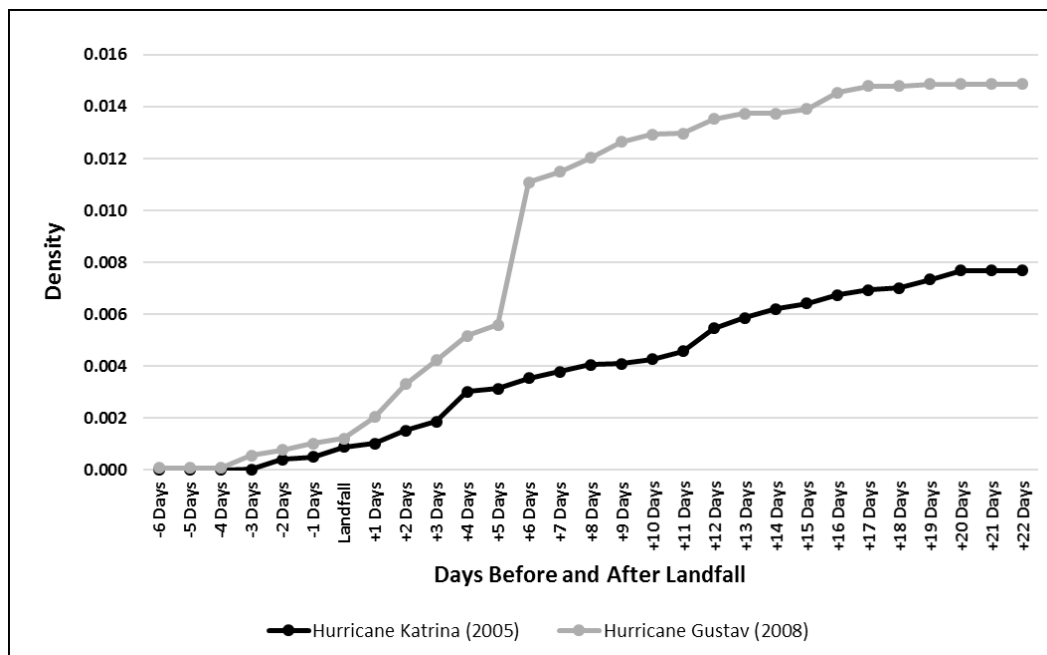


Figure 3: Comparison of Response Network Density by Day: Hurricane Katrina and Hurricane Gustav

The network density scores for Hurricane Rita and Hurricane Ike plotted over time are presented in Figure 4. Like the response networks in Louisiana, the overall density scores for the response networks in Texas were also low. For the Rita network, response organizations began to establish linkages with one another at least four days before landfall. By September 24, 2005, the density of the Rita network had reached 0.002633, which was the highest landfall density of all response networks. In contrast, on the day of landfall, the density of the Ike network was 0.000551, which was the lowest density of all response networks. The Rita data also indicate that six days after landfall, the density of the network increased from 0.004475 to 0.006055. On this date, Texas counties were operating supply stations, crews were working to remove debris from the streets and to restore electrical services, and FEMA opened a disaster recovery center. From a comparative basis, however, these data suggest

that the capacity of response organizations to become active decreased in the three years that followed Hurricane Rita.

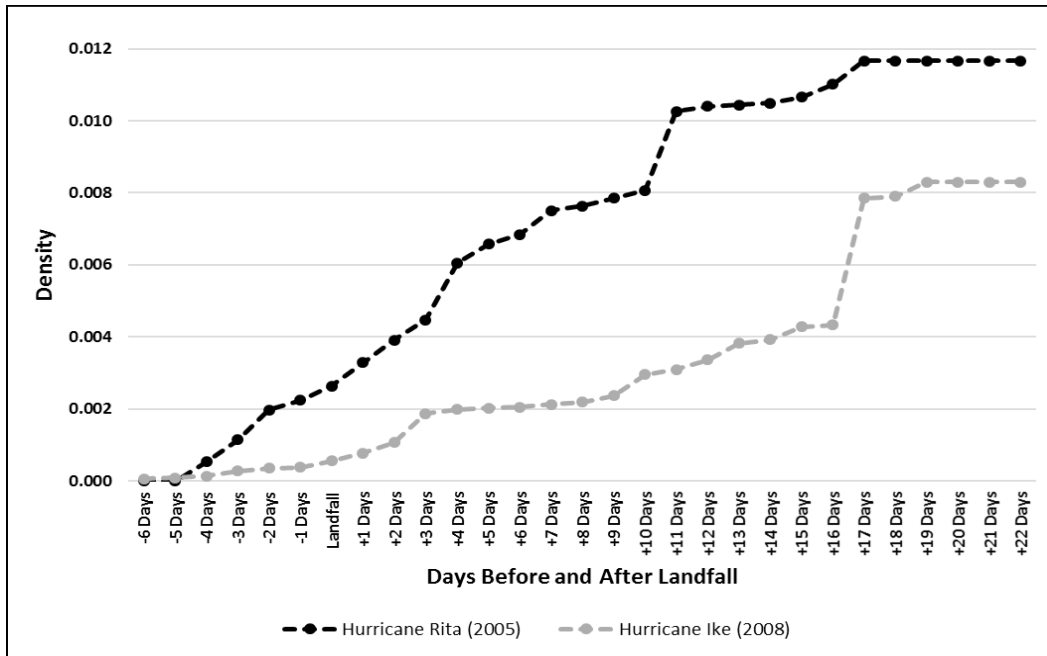


Figure 4: Comparison of Response Network Density by Day: Hurricane Rita and Hurricane Ike

Network Degree Centralization

For the next step in our structural analysis, we calculated network degree centralization statistics for each of the hurricane response networks. Figure 5 reports the network degree centralization scores for Hurricane Katrina and Hurricane Gustav plotted over time. These data indicate that the organizations in both response networks gradually became increasingly connected to one another. At the time of landfall, both the Katrina network and the Gustav network were similar in structure. The Katrina network, however, was slightly more centralized than the Gustav network, at 0.039761 and 0.030728 respectively. The next day, the Gustav network became more centralized than the Katrina network, a finding that would remain constant over the next twenty-one days.

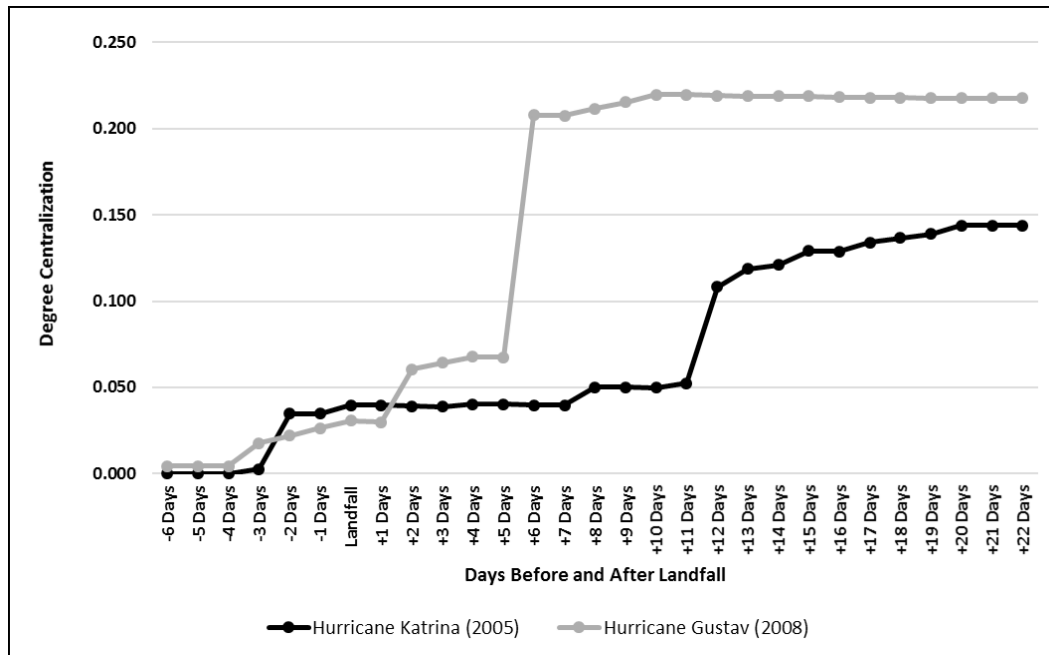


Figure 5: Comparison of Response Network Degree Centralization by Day: Hurricane Katrina and Hurricane Gustav

These data also reveal two points of structural change within these response networks. For the Rita network, the point of structural change occurred twelve days after landfall, when the network's degree centralization score increased from 0.052306 to 0.108327. This finding parallels the density finding discussed in the previous subsection of this article. A point of structural change occurred much earlier in the Gustav network, on day six, when the degree centralization score increased from 0.067421 to 0.207980. On this day, there were multiple interactions exchanged between response organizations. These interactions reflected the collective response of city, county and state firefighters to fight fires in Terrebonne Parish, the Louisiana Department of Homeland Security and Emergency Preparedness working with state and local officials to establish and manage aid centers, and agencies such as FEMA and the Louisiana Department of Social Services working to provide food and social services to aid centers and citizens.

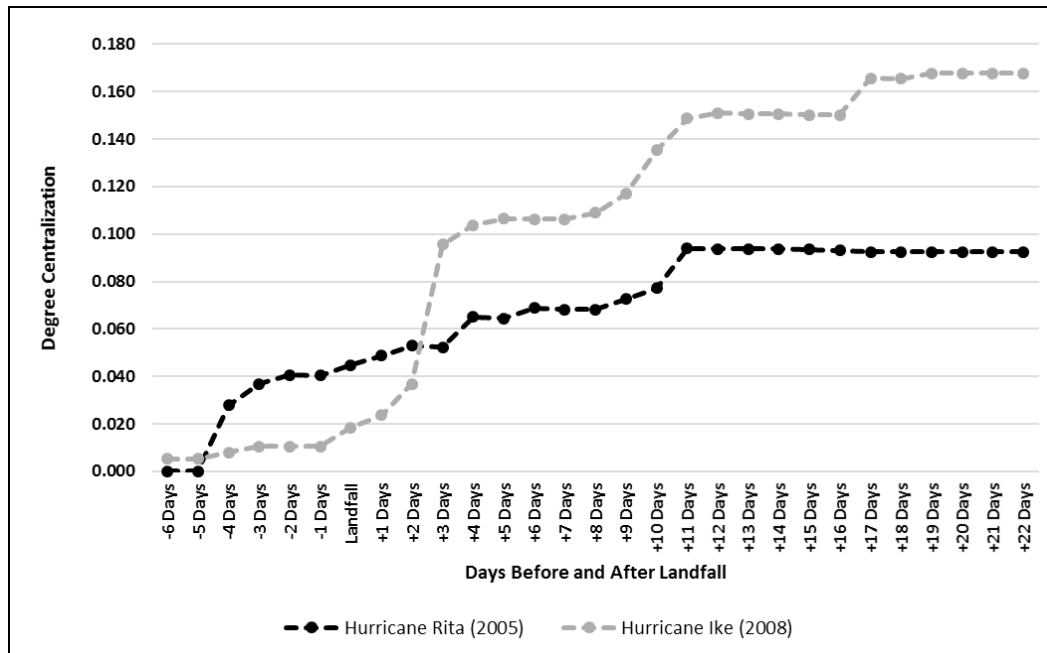


Figure 6: Comparison of Response Network Degree Centralization by Day: Hurricane Rita and Hurricane Ike

Finally, the network degree centralization scores for the Rita and Ike response networks, plotted longitudinally, are presented in Figure 6. Like the Katrina and Gustav networks, these data indicate that the organizations in both Texas response networks became increasingly connected. When Hurricane Rita came ashore, the storm's response network centralization score was 0.018416. Twelve days later, the network's centralization score reached 0.093897, its maximum level. In contrast, the Ike response network, which had a centralization score of 0.018416 when the storm came ashore, rapidly increased to 0.095680 three days later. Perhaps due to the size of the storm, the Ike network's centralization score continued to increase over the next few days, reaching 0.167801 nineteen days after landfall. From a comparative basis, the data presented in Figure 5 and Figure 6 suggest that the organizations in all four response networks structured their interactions in a way that generated increasing levels of centralization, but once a certain centralization threshold level was reached, the centralization processes began to stabilize.

Investments in Training and Technology Post-2005

For the final stage of our analysis, we reviewed disaster policy changes that occurred after 2005.⁴⁹ At the federal level, Congress strengthened the capacity of the federal government's disaster management system. In reaction to problems encountered after Hurricane Katrina, legislation such as the *Post-Katrina Emergency Management Reform Act of 2006* [Reform Act] reorganized the country's disaster management institutions, strengthened and expanded the collection and dissemination of information, and reinforced communication and coordination capacities.⁵⁰ The Reform Act also created the National Integration Center, which was charged to strengthen disaster management training and to promote collaboration among public, private, and non-profit organizations. Finally, the Reform Act required the Department of Homeland Security to modify its *National Emergency Communications Plan* so

that officials and disaster responders had the ability to communicate with one another after a disaster event.⁵¹

In Louisiana, the legislature amended the *Louisiana Homeland Security and Emergency Assistance and Disaster Act* (Disaster Act) in 2006.⁵² In doing so, the legislature modified the state's disaster management institutions, thereby improving their capacity to manage disaster events. The Disaster Act directed the Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP) to provide disaster management training and support throughout the state. The Disaster Act also established the state's Emergency Operations Center, which coordinates the state's emergency management operations. The Emergency Operation Center also assists local jurisdictions to coordinate response activities with their public, private and non-profit partners. Furthermore, the Louisiana legislature required the state's parishes to develop emergency response plans and directed GOHSEP to provide technical assistance to parish authorities to help them to develop these plans.⁵³ Finally, Louisiana spent more than US\$180 million to strengthen the Louisiana Wireless Information Network (LWIN).⁵⁴ Managed by GOHSEP and used by approximately 80,000 public and nonprofit personnel, the LWIN communication system can integrate with the communication networks used by neighboring states and maintain continuous communications in areas affected by disaster.

Finally, in Texas, the legislature also took steps to strengthen the state's disaster management capacities. These changes, which were not adopted until 2007 because the Texas legislature convenes on a bi-annual basis, were made to the *Texas Disaster Act of 1975*. These amendments required that all public officials receive at least three hours of disaster management training before they assume their duties. The amendments also mandated that the Emergency Management Director be the presiding officer of the governing body of a city or country. Finally, the amendments established the Texas Statewide Mutual Aid system, which sets the conditions under which local governments may assist each other without a written agreement. Like Louisiana, Texas communities sought to improve their disaster management capacities. Communities like Houston upgraded their communications systems, conducted training, and disseminated information to the public. Despite such investments, the state of Texas reported that, three years after Hurricane Ike, its public safety communications shortcomings had yet to be addressed.⁵⁵

Discussion

The findings generated by this study support the theoretical propositions that framed the analysis presented in this article. Our first proposition stated that a resilient disaster response network is comprised of a heterogeneous collection of organizations that interact with one another to pursue and obtain collective goals. This proposition is supported by the data presented in Tables 1 and 2. These tables indicate that public sector organizations from jurisdictions classified as county/parish or lower were the most prevalent in all four response networks. This finding not only reflects the idea that local agencies and officials are best positioned to respond to a disaster event, it also reflects the idea that communities in the United States expect their governments to deliver response assistance after a disaster. Moreover, these data indicate that federal and state organizations contributed to the response networks, often as coordinators or as the distributors of resources. More broadly, these data also indicate that private and nonprofit organizations participated in the response networks, bringing with them their resources and experience. Although their

participation was documented in different numbers, organizations from these sectors represented between 13% and 24% of all organizations identified in each response network. In the Rita network, for example, nonprofit organizations represented 16.65% of all identified organizations. In the Ike network, however, they represented 26.34% of the detected organizations. Despite these differences, which appear to be influenced by the scale of the disasters, the organizations identified in all four response networks had the potential to use each other to locate information, money, personnel and equipment, and if a relationship was established, to move these resources to where they were needed.

Proposition 2 asserted that a resilient disaster response network can adapt its structure in response to the uncertainties and complexities present in the changing operational environment. In terms of adaptation as measured by network growth, the data presented in Figure 1 and Figure 2 indicate that all four response networks experienced steady growth over time. For example, in Louisiana, approximately 25% of all organizations that were active by the date of landfall for both Hurricane Katrina and Hurricane Gustav. After landfall, the organizations in the Gustav network became active more quickly than those in the Katrina network. In Texas, the data suggest that the opposite occurred, as the 2008 response network, which formed after Hurricane Ike, became active more slowly than the 2005 response network, which formed after Hurricane Rita. In terms of network structure, the findings presented in Figures 3 through 6 also indicate that all four response networks underwent change. Perhaps the best example of structural change occurred in the Gustav response network, when six days after landfall, the degree centralization score increased from 0.067421 to 0.207980, a result of an increase in reported organizational interactions related to firefighting, the management of aid centers, and the distribution of relief resources. An additional finding, reported in Figure 4, is the identification of points of structural change in the later stages of the Rita and Ike response networks, which may represent the system shifting from the response phase to the recovery phase. If so, this finding supports the transitions documented in the response and recover processes that occur after disaster events in large urban areas.⁵⁶

The final proposition stated that information communication technologies (ICT), properly designed and implemented, facilitate the resilience of disaster response networks. The review of policy changes and investments in information technology revealed that steps taken at the federal level, and in the state of Louisiana, likely strengthened disaster resilience. At the federal level, Congress adopted the *Post-Katrina Emergency Management Reform Act of 2006*, which reorganized the country's disaster management institutions, strengthened disaster management training, promoted organizational collaboration, and required the Department of Homeland Security to modify its National Emergency Communications Plan. In Louisiana, the legislature amended the state's *Louisiana Homeland Security and Emergency Assistance and Disaster Act* in 2006. In doing so, the state directed GOHSEP to expand access to disaster management training, established the state's Emergency Operations Center, and required the state's parishes to develop emergency response plans. Central to these efforts was Louisiana's decision to strengthen the Louisiana Wireless Information Network, the system used to maintain communications in disaster areas. In contrast, although the Texas legislature did adopt disaster management legislation, the changes were minor, and many did not come into effect until the later part of 2007, leaving little time for officials to implement these changes before the arrival of Hurricane Ike. Equally important, despite recognizing that it needed to strengthen its communication infrastructure, Texas as a state did not appear to take sufficient action prior to the arrival of Hurricane Ike.

Viewed collectively, all four disaster response networks demonstrated structural change. These structural changes, however, did not occur at the same rate nor did they evolve in the same manner, which suggests that each response network sought to find the appropriate “fit” for the context in which it operated. While all four networks were activated in response to different events, these findings suggest that Louisiana managed to strengthen the capacities and processes that generate resilience. Although these findings are subject to further inquiry, they indicate why the organizational response to Hurricane Gustav was more robust than the organizational response to Hurricane Katrina. In contrast, in Texas, the results generated for the Rita response network suggest that the network was likely influenced by the observed consequences from Hurricane Katrina three weeks earlier, an event that reinforced the need for preparedness and response throughout Texas. As the memory of Hurricane Katrina began to fade, and in line with the consensus that the response to Rita was constrained by shortcomings in evacuation processes, Texas did not take substantial steps to improve its disaster response capacities after 2005. Consequently, the level of resilience dropped over the course of three years, which may explain the slower response of the Ike network in 2008, in comparison to the Rita response network.

Conclusions

In the context of disaster response networks, resilience represents a set of adaptive capacities and a set of adaptive processes. Tied together in a series of feedback loops that facilitate learning, these capacities and processes provide the organizations in a disaster response network the ability to overcome the uncertainties and complexities present in the post-disaster environment through adaptation and change. The findings from this analysis demonstrate that disaster response networks undergo structural change, as a large heterogeneous collection of response organizations come together, collect and disseminate information, and seek to identify and implement solutions to address rapidly the needs of those affected by the disaster event. Although each of the response networks analyzed—Hurricanes Katrina and Gustav in Louisiana and Hurricanes Rita and Ike in Texas—experienced structural change, the rate at which these changes occurred differed in each network. A review of the policy changes and investments in information technology made in Louisiana following Hurricane Katrina, in contrast to those undertaken in Texas, suggests why the Hurricane Gustav response network was more robust than the Hurricane Ike response network. The findings support the well-established proposition that sustained investments in information technology infrastructure support the development of resilience in disaster response networks.

For the organizations and government officials responsible for protecting the United States from the consequences of terrorist attacks, technological disasters, and catastrophic natural events, the challenge is to determine how to reduce risk in an environment that is becoming increasingly interdependent and risk prone. As we advance further into the twenty-first century, risk reduction efforts will become more difficult, as policy-makers seek the means to manage the effects of urbanization, population growth, environmental change, and technological advancement. The promotion of resilience in disaster response networks may provide communities with a cost-effective tool that could be used to manage the consequences of a variety of risks. This means that, from a public policy perspective, federal, state and local governments should continue to update their institutional arrangements to facilitate administrative flexibility, organizational collaboration and cooperation, and the use

of technology to share information across a heterogeneous community of organizations, decision-makers, and individual citizens.⁵⁷

In addition to strengthening administrative capacities within the United States, it is essential to develop a conceptual framework that outlines the parameters of network resilience for disaster response organizations. This framework needs to identify factors that promote adaptive capacity in disaster response networks, as well as indicators that facilitate the measurement and assessment of network resilience. As the findings from this study suggest, the components and indicators of network resilience likely relate to the design of institutional arrangements, use of information technology, development of coordination plans and mutual aid agreements, and systematic use of disaster management training. To increase network performance, it is essential to evaluate whether public investments for disaster preparedness and response operations are producing the expected results. Although the concept of resilience does not provide a set of actionable solutions for communities exposed to recurring risk, such investigations contribute to more informed administrative adaptation.⁵⁸

About the Authors

Thomas W. Haase received his Ph.D. from the Graduate School of Public and International Affairs at University of Pittsburgh. He is currently an Assistant Professor of Public Administration at the Department of Political Science at Sam Houston State University, where his teaching portfolio includes courses on international disaster management, community and social resilience, program evaluation, and Texas government. His research has focused on issues of disaster management, community resilience, and public administration education. He may be reached at twhaase@gmail.com

Güneş Ertan received her Ph.D. from the Graduate School of Public and International Affairs at University of Pittsburgh. She is currently an Assistant Professor of International Affairs at Koç University in Istanbul, Turkey where she teaches courses such as social networks and policy analysis. Her research focuses on the relationship between social networks and collective action. More specifically she studies the role of social networks in shaping collective action outcomes within the context of policy processes and social movements. She may be reached at gunesertan@ku.edu.tr.

Louise K. Comfort is Professor of Public and International Affairs and former director, Center for Disaster Management, University of Pittsburgh. She is a Fellow, National Academy of Public Administration, and author or coauthor of seven books, including *Designing Resilience: Preparing for Extreme Events* (University of Pittsburgh Press, 2010), *Mega-Crises* (Charles C. Thomas, 2012), and *The Dynamics of Risk* (Princeton University Press, forthcoming, 2018). Her primary research interests are in decision making under conditions of uncertainty and rapid change, and the uses of information technology to develop decision support systems for managers operating under urgent conditions. She has published articles on information policy, organizational learning, and sociotechnical systems, and serves as the Social Science Editor for *Natural Hazards Review*. She may be reached at comfort@gspia.pitt.edu.

Acknowledgements

The authors would like to acknowledge that support for this research was received from the National Science Foundation, Grant #0729456: DRU: Designing Resilience for Communities at Risk: Improving Decision Making to Support Collective Action under Stress, 9/1/2007–8/31/2012, the Graduate School of Public and International Affairs, University of Pittsburgh, and the College of Humanities and Social Sciences, Sam Houston State University. We are also grateful for the constructive comments received during the 10th Annual Homeland Defense/Security Education Summit, held at George Mason University on March 23rd and 24th, 2017.

Notes

- 1 United States and Department of State, *National Security Strategy: 2010*, (Washington, DC: The White House, U.S. Department of State, 2010), <http://nssarchive.us/national-security-strategy-2010/>. The full report, *Disaster Resilience: A National Imperative*, is published by the National Academies Press, Washington, DC, 2012.
- 2 Department of Homeland Security, "Quadrennial Homeland Security Review: 2014" (Washington DC: Department of Homeland Security, 2014), <https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>.
- 3 Federal Emergency Management Agency, *2015 National Preparedness Goal* (Washington DC: Federal Emergency Management Agency, 2015), 1, <https://www.fema.gov/media-library/assets/documents/25959>.
- 4 William N. Dunn, *Public Policy Analysis: An Introduction*, 5th ed. (New York, N.Y.: Routledge, 2016).
- 5 Donald F. Kettl, *The Transformation of Governance: Public Administration for the Twenty-First Century America* (London, England: John Hopkins University Press, 2002).
- 6 Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York, N.Y.: Basic Books, Inc., 1984).
- 7 Raanan Lipshitz and Orna Strauss, "Coping with Uncertainty: A Naturalistic Decision-Making Analysis," *Organizational Behavior and Human Decision Processes* 69, no. 2 (February 1, 1997): 149–63.
- 8 Elinor. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge, Massachusetts: Cambridge Univ. Press, 2005), 48–49.
- 9 Naim Kapucu et al., "Interorganizational Network Coordination under Stress Caused by Repeated Threats of Disasters," *Journal of Homeland Security and Emergency Management* 7, no. 1 (January 30, 2010).
- 10 Louise K. Comfort, "Crisis Management in Hindsight: Cognition, Communication, Coordination, and Control," *Public Administration Review* 67, no. 1 (2007): 189–197.
- 11 Louise K. Comfort, "Designing Policy for Action: The Emergency Management System," in *Managing Disaster: Strategies and Policy Perspectives*, ed. Louise K. Comfort (Durham: Duke University Press Books, 1988), 3–21; Louise K. Comfort, *Shared Risk: Complex Systems in Seismic Response* (New York, N.Y.: Pergamon, 1999); Comfort, "Crisis Management in Hindsight"; Qian Hu and Naim Kapucu, "Information Communication Technology Utilization for Effective Emergency Management Networks," *Public Management Review* 18, no. 3 (March 15, 2016): 323–48; Bruce Cutting and Alexander Kouzmin, "From Chaos to Patterns of Understanding: Reflections on the Dynamics of Effective Government Decision Making," *Public Administration* 77, no. 3 (1999): 475–508; Louise K. Comfort, Arjen Boin, and Chris C. Demchak, eds., *Designing Resilience: Preparing for Extreme Events*, vol. 90, 2 vols. (Pittsburgh, Pa: University of Pittsburgh Press, 2010).
- 12 These four hurricanes are explored in greater detail in a separate working paper that investigates the nature of the cross-jurisdictional linkages that formed between disaster response organizations after each hurricane event. Comfort, Louise, Thomas W. Haase and Gunes Ertan (2017) *The Dynamics of Change Following Extreme Events: Shattered Communities, Emergent Networks, and Sustainable Resilience* (unpublished).
- 13 Aaron Wildavsky, *Searching for Safety, Social Theory and Social Policy* (New Brunswick: Transaction Press, 1988), 77, <http://www.transactionpub.com/title/978-0-912051-18-5.html>.
- 14 Comfort, *Shared Risk: Complex Systems in Seismic Response*, 21.
- 15 Susan L. Cutter, "The Landscape of Disaster Resilience Indicators in the USA," *Natural Hazards* 80, no. 2 (January 2016): 741–58; Susan L. Cutter et al., "A Place-Based Model for Understanding Community Resilience to Natural Disasters," *Global Environmental Change-Human and Policy Dimensions* 18, no. 4 (October 2008): 598–606; Patricia H Longstaff et al., "Building Resilient Communities: A Preliminary Framework for Assessment," *Homeland Security Affairs* 6, no. 3 (September 2010). \u0022Global Environmental Change-Human and Policy Dimensions\u201c 18, no. 4 (October 2008).

- 16** Ashley D. Ross, *Local Disaster Resilience: Administrative and Political Perspectives*, Routledge Research in Public Administration and Public Policy (New York: Routledge, 2013).
- 17** Michael McGuire, "Collaborative Policy Making and Administration: The Operational Demands of Local Economic Development," *Economic Development Quarterly* 14, no. 3 (2000): 278.
- 18** Jan Kooiman, *Modern Governance: New Government-Society Interactions* (London: Sage, 1994); Donald F. Kettl, *System under Stress: Homeland Security and American Politics* (Washington, D.C.: CQ Press, 2004).
- 19** Comfort, *Shared Risk: Complex Systems in Seismic Response*; Louise K. Comfort and Thomas Haase, "Communication, Coherence, and Collective Action: The Impact of Hurricane Katrina on Communications Infrastructure," *Public Works Management & Policy* 10, no. 4 (April 1, 2006): 328–43.
- 20** Keith G. Provan and Patrick Kenis, "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory* 18, no. 2 (April 1, 2008): 229–52, doi:10.1093/jopart/mum015.
- 21** *Ibid.*, 229.
- 22** William L. Waugh and Gregory Streib, "Collaboration and Leadership for Effective Emergency Management," *Public Administration Review* 66, s1 (2006): 131–140.
- 23** Naim Kapucu, "Interorganizational Coordination in Dynamic Context: Networks in Emergency Response Management," *Connections* 26,2 (2005): 33–48.
- 24** Robert Axelrod and Michael D. Cohen, *Harnessing Complexity: Organizational Implication of a Scientific Frontier* (New York, N.Y.: Basic Book, Inc., 2000); Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex* (New York, N.Y.: W. H. Freeman and Company, n.d.); John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Reading, Mass.: Addison-Wesley Pub. Co., 1995).
- 25** John H. Holland, *Hidden Order: How Adaptation Builds Complexity* (Reading, Mass.: Addison-Wesley Pub. Co., 1995)
- 26** John H. Holland, *Signals and Boundaries: Building Blocks for Complex Adaptive Systems* (Cambridge, Massachusetts: MIT Press, 2014).
- 27** Axelrod and Cohen, *Harnessing Complexity: Organizational Implication of a Scientific Frontier*, 9.
- 28** Axelrod and Cohen, *Harnessing Complexity: Organizational Implication of a Scientific Frontier*.
- 29** *Ibid.*
- 30** *Ibid.*, 156.
- 31** Hu and Kapucu, "Information Communication Technology Utilization for Effective Emergency Management Networks."; Naim Kapucu, "Interorganizational Coordination in Dynamic Context: Networks in Emergency Response Management," *Connections* 26, no. 2 (2005): 33–48; Comfort, "Crisis Management in Hindsight."; Comfort and Haase, "Communication, Coherence, and Collective Action."
- 32** Louise K. Comfort et al., "Designing Adaptive Systems for Disaster Mitigation and Response: The Role of Structure," in *Designing Resilience: Preparing for Extreme Events*, ed. Louise K. Comfort, Arjen Boin, and Chris C. Demchak (Pittsburgh, Pa.: University of Pittsburgh Press, 2010), 349.
- 33** Albert Charns, "The Principles of Sociotechnical Design," *Human Relations* 29, no. 8 (1976): 783–89.
- 34** Herbert A. Simon, *The Sciences of the Artificial*, 3. ed., [Nachdr.] (Cambridge, Mass.: MIT Press, 2008); Herbert A. Simon, "The Architecture of Complexity," *General Systems* 10, no. 1965 (1965): 63–76.
- 35** Elayne Coakes, *Knowledge Management in the Sociotechnical World: The Graffiti Continues* (London: Springer, 2002).

- 36** Ramesh R. Rao, Jon Eisenberg, and Ted Schmitt, eds., *Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery* (Washington D.C.: National Research Council of the National Academies, 2007), <http://nap.edu/11842>.
- 37** William L. Waugh and Gregory Streib, "Collaboration and Leadership for Effective Emergency Management," *Public Administration Review* 66, no. s1 (2006): 131–140; Comfort, "Crisis Management in Hindsight."; Donald P. Moynihan, "Learning under Uncertainty: Networks in Crisis Management," *Public Administration Review* 68, no. 2 (2008): 350–365; D. P. Moynihan, "The Network Governance of Crisis Response: Case Studies of Incident Command Systems," *Journal of Public Administration Research and Theory* 19, no. 4 (October 1, 2009): 895–915; Carter T. Butts, Ryan M. Acton, and Christopher Marcum, "Interorganizational Collaboration in the Hurricane Katrina Response," *Journal of Social Structure* 13, no. 1 (2012); Naim Kapucu, *Multi-Agency and Cross-Sector Coordination in Response to Disasters: The World Trade Center Attack in New York City, September 11, 2001* (LAP Lambert Academic Publishing, 2009); Kapucu, "Interorganizational Coordination in Dynamic Context."; Comfort and Haase, "Communication, Coherence, and Collective Action." September 11, 2001 (LAP Lambert Academic Publishing, 2009).
- 38** U.S. House of Representatives, "A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina" (Washington D.C.: U.S. Government Printing Office, 2006), http://katrina.house.gov/full_katrina_report.htm.
- 39** National Hurricane Center, "Tropical Cyclone Report: Hurricane Gustav," (National Hurricane Center, September 9, 2014), www.nhc.noaa.gov/data/tcr/AL072008_Gustav.pdf.
- 40** National Weather Service, "Post Storm Data Acquisition: Hurricane Rita," November 14, 2005, www.nws.noaa.gov/om/data/pdfs/Rita.pdf.
- 41** National Hurricane Center, "Tropical Hurricane Report: Hurricane Ike" (National Hurricane Center, February 4, 2009), www.nhc.noaa.gov/data/tcr/AL092008_Ike.pdf.
- 42** Ibid.
- 43** Edward O. Laumann, Peter V. Marsden, and David Prensky, "The Boundary Specification Problem in Network Analysis," in *Research Methods in Social Network Analysis* (Transaction Publishers, 1983), 22–32.
- 44** Federal Emergency Management Agency, "National Response Plan" (Washington D.C.: Department of Homeland Security, 2004), <http://www.au.af.mil/au/awc/awcgate/nrp/plan.pdf>.
- 45** Federal Emergency Management Agency, "National Response Framework," (Washington, D.C: Department of Homeland Security, 2008), <https://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.
- 46** Steven P. Borgatti, Martin G. Everett, and Linton C. Freeman, *Ucinet for Windows: Software for Social Network Analysis* (Harvard, MA: Analytic Technologies, 2002), <https://sites.google.com/site/ucinetsoftware/home>.
- 47** Stanley Wasserman and Katherine Faust, *Social Network Analysis: Methods and Applications*, Structural Analysis in the Social Sciences 8 (Cambridge, Massachusetts: Cambridge University Press, 1994), 101.
- 48** Ibid., 180.
- 49** The policy changes and their potential impact on the disaster response activities that occurred in Louisiana and Texas after Hurricane Gustav and Hurricane Ike in 2008 are explored in greater detail in a separate working paper. This working paper investigates the nature of the cross-jurisdictional linkages that formed between disaster response organizations after each hurricane event. Comfort, Louise, Thomas W. Haase and Gunes Ertan (2017) *The Dynamics of Change Following Extreme Events: Shattered Communities, Emergent Networks, and Sustainable Resilience* (unpublished).
- 50** Post-Katrina Emergency Management Reform Act, *Pub. L. No. 109-295, 120 Stat. 1355*, 2006.
- 51** Ibid.
- 52** Governor's Office of Homeland Security and Emergency Preparedness, "A Decade After Hurricanes Katrina and Rita – 10 Initiatives That Make Louisiana Smarter + Safer + Stronger + More Resilient." (Baton

Rouge, LA: Governor's Office of Homeland Security and Emergency Preparedness, 2015), <http://gohsep.la.gov/recover/katrina-rita-10-years-later>.

53 Ibid., 12.

54 Ibid., 14–15.

55 Texas Department of Public Safety, "Texas Department of Public Safety Report on Interoperable Communications to the Texas Legislature," (Austin, Texas: Texas Department of Public Safety, August 31), www.dps.texas.gov/LawEnforcementSupport/communications/interop/documents/interopRpt.pdf.

56 Vale J. Lawrence and Thomas J. Campanella, "Resilience Axioms," in *In the Resilient City: How Modern Cities Recover from Disasters*, ed. Vale J. Lawrence and Thomas J. Campanella (Oxford, United Kingdom: Oxford University Press, 2005), 335–55.

57 Joseph W Pfeifer, "Network Fusion: Information and Intelligence Sharing for a Networked World," *Homeland Security Affairs* 8, no. 1 (2012).

58 Ann Marie Thomson and James L. Perry, "Collaboration Processes: Inside the Black Box," *Public Administration Review* 66, no. s1 (2006): 20–32.

Copyright © 2017 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).

Protecting the Right to Be an American: How Pennsylvanians Perceive Homeland Security

Alexander Siedschlag

Introduction

Homeland Security is strategically defined as an enterprise based on a concerted national effort: a nation-wide comprehensive activity, including all of government across federal, state, local, territorial and tribal tiers; the public and the private sector; and the whole community of first responders and vigilant citizens. While Homeland Security in addition to government agencies and the private sector counts on each single citizen as part of the whole-community approach, little is known about how it actually resonates with citizens. In fall 2016, as part of a representative phone poll (the Penn State Omnibus Poll), Pennsylvania residents' perception of Homeland Security was assessed.

How Citizens Define Homeland Security

A clear majority of Pennsylvanians (65%) define Homeland Security as something of positive value that provides needed protection to U.S. citizens. This matches nation-wide poll data on citizens' approval ratings of the Department of Homeland Security. Only a minority (7%) see it as something negative, citing surveillance and infringement of liberty, huge bureaucracy, or waste of taxpayers' money as reasons. Not a lot of Pennsylvanians are aware that Homeland Security actually transcends the federal level of government.

What Homeland Security Protects From

Not many but at least 16% of Pennsylvanians are aware of the all-hazards approach to Homeland Security and that its mission space extends beyond preventing terrorism. There are in fact five Homeland Security core missions. The founding core mission of Homeland Security, "Preventing Terrorism and Enhancing Security" is cited by more than a third (37%) of Pennsylvanians. Not as much awareness exists for the other four core missions. In any case, 12% cite the core mission of "Securing and Managing Our Borders," whereas only 4% refer to the core mission of "Enforcing and Immigration Laws." That "Safeguarding and Securing Cyberspace" and "Ensuring Resilience to Disaster" are Homeland Security core

missions is largely unknown to Pennsylvanians. Yet nearly a quarter (23%) see an additional main mission in Homeland Security: Ensuring general safety, wellbeing of the people, and protection from violence as such.

Who Provides Homeland Security

The majority of Pennsylvanians (63%) see Homeland Security provided for by the federal government. At the same time, 17% recognize that the Commonwealth of Pennsylvania is involved in providing Homeland Security to the citizens. The concept of the whole-community approach only has reached a few: Just 1% refer to collaboration among several actors beyond the federal government, and those who do most often cite police as an example, followed by airlines.

How Homeland Security Affects Daily Life

Potentially, Homeland Security affects or even involves citizens on a daily basis. Examples would be suspicious activity reporting, as encouraged through the “If You See Something, Say Something” campaign, cyber security awareness, or active shooter preparedness. Most Pennsylvanians (70%) yet are not sure about the effect of Homeland Security on their daily lives. However, almost a quarter (23%) feel Homeland Security to affect their daily lives – such as by ensuring safe and secure neighborhoods; via the Transportation Security Administration (TSA) when travelling on a plane, through security precautions in public transportation; or by encouragement to report suspicious activity.

Conclusion and Recommendations

Pennsylvanians appreciate homeland security as something that the country does to protect the American way of life and the safety of American citizens. No more than a few are aware that they themselves, as citizens, are part of the Homeland Security Enterprise. Increased citizen-involvement campaigns are needed, and should be placed within a common framework to increase homeland security recognition consistent with the whole-community approach. National campaigns such as “See Something, Say Something,” State campaigns such as “Ready.pa,” and sector-specific safety and security campaigns such as for example in the public transportation sector should be candidates for visible co-branding with U.S. Homeland Security to place them into a strategic citizen-involving context. Further, as we are moving towards the 2018 Quadrennial Homeland Security Review, a bottom-up review perspective should be included that addresses State-level information, such as empirical analysis of citizens’ risk perception, understanding of, and expectations in the Homeland Security Enterprise.

Alexander Seidschlag may be reached at aus50@psu.edu

Mass Migration and the Media: Convergence and Divergence of Global Media Narratives Towards a Working Model

by Emily Damm, Amy Jones, Skye Cooley, and Elizabeth Roshelli

The size and scope of the Syrian refugee crisis has made it a salient humanitarian crisis for the international community that has given rise to fears among European and U.S. populations and leaders, altered the demographic landscape of the Middle East and Europe, and exposed a generation of youth to lives as exiles. Our quantitative, inductive content analysis analyzed news media coverage of refugees from Arabic, Russian, and American media news sources in an attempt to understand how the crisis has been packaged and presented to citizens across the globe in order to give insight to the motives and potential actions to be taken by the global community concerning the crisis. The study was conducted using the M3S media monitoring system at Texas A&M University. The M3S technology allows researchers to evaluate foreign language news broadcast and media websites in the original context with validated English language translations.

The authors evaluated *Al Jazeera (Arabic)*, *Rossiya 24 (Russian)*, and *The New York Times (U.S)* as sources for analysis. The research was conducted within the timeframe of August 5 to 21, 2016, as that time spanned the 2016 Olympics in Rio, Brazil, in which the creation of the Olympic Refugee team caused a spike in media discussion of the refugee crisis. A total of 193 articles were coded across the three news sources using the keyword "Refugee." Researchers developed a coding scheme of ten categories designed to give insight into presentation of refugees in media [see table1.]. The coded data was then evaluated for statistical significance between the news sources.

The findings showed the three media outlets to be apathetic towards refugees, with no attempt at humanizing those affected by the crisis. Little discussion was given to physical, educational, and/or psychological harm being done to refugees. The media outlets also gave very few opportunities for the refugees to speak in their own voice, and instead crafted stories around them as a mass entity. Media outlets were more likely to place blame on other governments for the crisis, rather than calling for or seeking an international political solution; none of the media outlets discussed solutions to the crisis as urgently needed. A few mentions of successful assimilation were given, typically in reference to the refugee athletes in the Olympics.

Rossiya 24 gave no mention of a political solution for the crisis and had the highest number of stories dehumanizing refugees; specifically relating refugees to acts of terrorism, crime, and an overall threat to Russian culture. Of particular note, the Russian media source was most likely to call for humanitarian aid from other nations to address the crisis.

Al Jazeera mentioned the mistreatment of refugees, discussed the crisis as a political event, and made calls for a solution in Syria more than any other source. Most often these stories focused on the impact refugees had on neighboring countries, researchers speculate this focus is due to the proximity of the crisis compared to the other media sources.

The New York Times focused on the crisis as a “foreign” event with little threat to U.S. culture. These stories typically made calls for US citizens to be accepting of refugees and had the highest number of stories with a humanizing component for refugees. *The New York Times* had the least number of stories calling for humanitarian aid or mention of refugee mistreatment.

While the findings were limited by the selected news outlets studied and narrow time frame, the snapshot of coverage offers insight toward the refugee crisis and demonstrates the ability of new technology that allow social scientist to monitor media message movements through global media. Such applications can allow for the modeling of global media and pave the way for new media theories. The lead author may be reached at emilybelledamm@gmail.com.

The State of Science Regarding Membership in Terrorist Organizations and Perpetration of Terrorist Attacks

by Sarah L. Desmarais, Joseph Simons-Rudolph,
Christine Shahan Brugh, Eileen Schilling, & Chad Hoggan
North Carolina State University

Background

One strategy in the fight against terrorism involves identifying individuals who are at heightened risk of joining terrorist organizations or perpetrating terrorist attacks. Success of this counterterrorism strategy will depend upon knowledge of the factors that increase risk for these outcomes. To date, the intelligence community has served as a primary source of information on terrorist organizations and activity. However, hundreds of scientific papers have been written on the topic and may offer important insights into risk factors for terrorism. These largely academic endeavors have been diverse in their foci, approach, and findings. As such, there is a need to summarize the state of science regarding membership in terrorist organizations and perpetration of terrorist attacks towards the goal of informing counterterrorism strategy.

Purpose

The purpose of this study was to conduct a systematic review of the published and unpublished scientific literature regarding factors associated with joining terrorist organizations or perpetrating terrorist attacks. Our primary research aims were to: 1) describe the characteristics of the scientific literature on risk factors for terrorism; and 2) to identify individual and environmental factors that are associated with membership in terrorist organizations and perpetration of terrorist attacks. We additionally explored the evidence supporting factors associated with the process of radicalization, including motivation and process.

Methods

Records were identified through searches of six abstracting and indexing databases using the following combinations of search terms: (a) terror* member*, (b) terror* affiliat*, (c)

terror* radical*, and (d) predict* terror*. Inclusion criteria were: (a) discussed the prediction of terrorism; addressed variables related to joining terrorist organizations or perpetrating terrorist attacks; reported in peer-review journals, dissertations, theses, conference presentations, government reports, or book chapters; (d) written in English (or reliable translation); and (e) produced between 1990 and 2015. We reviewed the reference sections of articles selected for inclusion for records that were not identified through these search strategies. In total, 205 articles met our inclusion criteria. Articles were coded by two researchers using a coding scheme; a subset of 19 articles were coded by both to establish inter-rater agreement.

Overview of Findings

Findings of our systematic review revealed a growth in scientific interest in terrorism over time: more than three-quarters of the articles were produced in the last 10 years. More than half were produced by authors in the United States. Across various aspects of terrorism (such as ideology, specific organizations, types of terrorists, or types of attacks), articles rarely specified the focus of their investigation. Instead, articles often treated terrorism as one unitary or homogenous construct. Most articles discussed theoretical perspectives, critiques, or case studies. The vast majority (81%) cited findings reported in other articles as their data source. There were just 50 articles that presented results of new empirical research.

Results of the 50 empirical articles were most frequently descriptive in nature, presenting the frequencies of various characteristics amongst a group of known terrorists. A handful of articles statistically compared characteristics between known groups of terrorists; for instance, comparing level of education or prevalence of criminal histories amongst one group of terrorists versus another. Only six articles presented findings of statistical comparisons between a group of known terrorists and a group of non-terrorists. As a result, empirical evidence of variables that discriminate between terrorists and non-terrorists is limited.

Analysis of the results reported in the empirical articles revealed nine variables with at least some evidence supporting for their relevance to terrorism. These include: age, socioeconomic status, prior arrest, education, employment, relationship status, having a grievance (political or personal), specific geographic region, and type of geographic area (i.e., urban or rural). Young age, low socioeconomic status, at least high school education, and unemployment showed statistically significant associations with terrorism outcomes when comparisons were conducted between known terrorists and non-terrorists. Findings also suggest that a triggering event, such as a major personal loss, may act as the impetus for radicalization. Additional individual characteristics, including country of birth, being Muslim, military experience, foreign travel history, family or friend in a terrorist or extremist organization, and environmental characteristics, including income inequality, and media and government influences, were prevalent among the samples of known terrorists and merit further investigation as potential risk factors. Given the limitations of the research, however, there is not enough empirical evidence to conclude that any of these variables are indeed *risk factors* for terrorism.

Recommendations

Findings of our review have implications for research and counterterrorism strategy. With respect to research, the small number of comparison studies is a critical limitation of the scientific literature. For a certain characteristic to be established as a risk factor for terrorism, it must be shown that the characteristic is statistically associated with terrorism and that it precedes (temporally) terrorist activity. It is only possible to show this statistical association through longitudinal studies that compare characteristics of terrorists and non-terrorists. As such, the conduct of comparative studies of individuals or groups over time is an urgent direction for future research. Further, articles typically focused on the independent effects of individual or environmental factors; yet, risk for terrorism most likely reflects an interaction of factors within and across these levels. We also were limited to examination of findings reported in the scientific literature to date. As new terrorist organizations emerge, there will be a need to revisit the relevance of established and refuted risk factors to these new threats.

With respect to counterterrorism strategy, our findings suggest that some presumed risk factors are not related to terrorism at all or in the anticipated direction. Take country of birth, for example; the one statistical comparison found that homegrown terrorists were more likely to be born in the United States than were their non-terrorist counterparts. Thus, domestic (as opposed to foreign) country of birth appears to be a risk factor for terrorism. Several other characteristics, such as religious conversion, being Muslim, and foreign travel history, were not statistically associated with terrorism outcomes, when examined. Counterterrorism strategies focused on these presumed risk factors are likely to be ineffective. Focusing on these factors also may increase risk for terrorism by contributing to a sense of persecution or discrimination that may (further) radicalize the individual or group and 'justify' terrorist activity. Finally, counterterrorism strategy that focuses on the presence of certain risk factors in and of themselves is likely to be of limited value without information on the social or political context and vice versa. To demonstrate, focusing on young age, male gender, and being single as risk factors for terrorism will not help discriminate amongst a pool of potential targets who are all young, single men. The lead author may be reached at sdesmarais@ncsu.edu.

Preparing for the Next Mass Migration: Lessons from the Past and Recommendations for the Future

by Dr. R. B. Watts

In 1995 over 60,000 migrants from both Haiti and Cuba attempted to reach the United States through maritime means, primarily vastly overcrowded sailboats and rafts. While it is unclear how many died in the attempt to reach the United States, the vast number were rescued via a huge inter-agency effort led by the Coast Guard and Navy. In 2006, it was feared that a migration on this scale was imminent due to failing health of President Castro. But much had changed since the 1990s; the strategic migration plan—Operation Vigilant Sentry—did not reflect the formation of DHS or the massive organizational and interagency shift that had occurred since 9/11. After an extensive inter-agency planning effort, the strategy was updated to reflect the new operational reality; fortunately, the threat of a new mass migration subsided.

Ten years later, the problem of maritime migration not only remains likely in our hemisphere due to political and economic unrest in South and Central America, but is also becoming a global phenomenon.

The History

Maritime migration has always been a consistent, global historical norm. This is perfectly understandable; the sea is the great global highway, and transport of goods and people on the sea is universal. The United States has experienced three mass migrations in the past 30 years, the size and scope of which are indicative of the problem; almost 200,000 migrants were rescued. Strategically, these events shared a number of common characteristics. Each was predicated by a significant political event, either the change (or perceived) change of policy by national governments or potential host nations. In each, migrant groups en masse perceived an opportunity for exploitation. Although this perception was often false (such as the rumor that the U.S. was changing its stance on accepting migrants, a significant driver in Haiti in 1994), the result was still the same. In general migrants were poor and almost completely ignorant or unaware of seafaring, creating an enormous safety of life at sea issue.

The Lessons

The overwhelming number of lessons learned during the mass migrations of the 1990s focused on effective command and control and the rapid establishment of a strategic process that effectively handled each phase of the migrant process (interdiction, transport, disposition). A centralized interagency command and control system, ideally at sea, was essential to migrant interdiction and rescue. This was effective in three areas:

Interdiction: Strategic interdiction is all about getting as many afloat assets to the region as quickly as possible. But simply “flooding” the area with assets wasn’t enough. During the Haitian and Cuban migrations this was conducted through the implementation of the “CTU” (Commander Task Unit) concept, a modification of the Navy Task Force model tailored for drug and migrant interdiction, an effective planning and execution organization for interagency support.

Transport: The number of people in danger and the speed required to rescue them often resulted in mass overloading; in one case, for example, a 270ft ship had well over 800 migrants onboard before it was forced to leave the area. This mass overloading was the norm rather than the exception. To address this, the CTU designated the largest afloat asset available—in this case, a Navy amphibious ship—to act as a roaming “bus” in the OpArea to load on migrants from rescue units who could then continue operations. This tactic was subsequently institutionalized in the follow on migrant plan for 2006.

Disposition: The 1990s mass migrations relied on GTMO for the disposition of migrants; as noted, camps where migrants could be housed and fed until final status was determined. Logistically, this was an enormous effort, coordinated by the establishment of a Joint Task Force (JTF) specifically designed to house, feed, and provide medical care for tens of thousands of migrants. This ultimately was a great success. However, it should be noted that the establishment of facilities at GTMO was a political decision and by far the most important one in terms of long term success.

The Future

These lessons were ultimately updated in the new migrant plan, Operations Vigilant Sentry (OVS) in 2007. But today, there are significant “game changers” that must be considered. These are primarily technological; in 1994 forces assigned for rescue and interdiction had the vast technological edge in the OpArea in terms of speed, mobility, and the ability to conduct command, control and communication. This is no longer the case. Today smugglers can coordinate with speed and sophistication previously undreamed of, including communication, navigation, and ability to control “battle rhythm through the internet.

Given the speed inherent in a mass migration and its potential scope, it is imperative that supply and training for a mass migration be part of the planning cycle and TTP (training, tactics and procedures) for today’s fleet of Coast Guard and Navy vessels. Rescue of migrants is a dangerous operation, and transport of large numbers of migrants must be designed and practiced by each class of vessel. Vessels of all services must have a fundamental understanding of the mechanics of mass migration as it is highly likely that literally anything

that floats will be sent to the scene of disaster. Readiness at the tactical level is key for overall success.

Ultimately, we must be familiar with our strategy and work to keep it current with modern trends. Predicting the future is, of course, the classic challenge for any strategist. But analyzing the classic elements of mass migration can be of great benefit. We know that migration by sea is becoming increasingly common in areas of political instability. We know that mass migration is often driven by rumor and conjecture, something that is easily spread through the internet. And we know that, in general, most nations are willing to address it if there is a unifying goal of saving life at sea. This should be our focus. The author may be reached at WattsR3@ndu.edu.

Community Resilience for Emerging Threats

Mary Tyszkiewicz

Abstract

Community resilience can be created via small group practices to respond to emerging threats, like accidents, disasters and terrorist emergencies. My case study research shows that that innovation happens when people care and connect in small groups of 16 or fewer in life-threatening situations. This natural process I found is described as the five-step Heroic Improv Cycle (Alert, Ready, Connect, Focus and Move), which describes how people work together to respond to emerging threats. I developed a training program called Heroic Improv to help small groups practice the abilities they need for high-stakes crises in a low-stakes practice. The Heroic Improv exercises are based on theater improvisation activities and have been tested with hundreds of participants in the U.S. and the Philippines. The Heroic Improv program is time-efficient, inexpensive and effective to prepare communities for emerging threats. The author may be reached at dr.marytysz@gmail.com

Evaluating Federal Grant Programming to Support State and Local Critical Infrastructure Protection: Results and Perspectives of Qualitative-Empirical End-User Survey Research in the EU

by Andrea Jerković

This paper presents the approach and main results of a series of surveys and foresight activities at Member State and EU levels to contribute to program evaluation and evolution by identifying end-user and practitioner technology and knowledge needs for improved critical infrastructure protection at state and local levels. The approach was first used in a study to support the Austrian Security Research Program KIRAS, launched in 2005 as the first Security Research Program in the EU, and then at the KIRAS grant project level. Subsequently, it was expanded on and used in European Union-co-funded Security Research projects. This included foresight projects such as FOCUS, where inter-project collaboration was established with DHS Science & Technology projects as well as with the FEMA Strategic Foresight Initiative.

Research has shown that homeland security can significantly benefit from actively seeking international best practices and an international scope on its mission space. While national specifics remain (such as the challenge of aged infrastructure in the U.S. and the EU focus on energy and transport sectors), main characteristics converge across the U.S. and the EU as well as its Member States, such as the private sector as the main owner of, and investor in, critical infrastructure. Both U.S. critical infrastructure and EU Member States National Critical Infrastructure (NCI) are commonly referred to as being to 85 percent in the hands of the private sector. Review and exchange of practices appear promising, in particular as the U.S. Homeland Security Enterprise and the EU's move towards a genuine Security Union have specific challenges in common that include converging mission spaces, the distributed character of the effort, its reaching across different horizontal and vertical tiers of government, as well as the objective of a security community, where all parts of society should be involved in the production of security as a public good, and be able to consume it.

In particular, federal programming in homeland and civil security should contribute to empowering actors at state and local levels to reach their mission goals, while fostering state and local ownership. Further, national risk management doctrine used to prioritize preparedness and response resources should consistently include risk assessment at state, local, territorial, and tribal levels, and systematically collect related expectations in homeland security policies and programs.

Overall, in order to effectuate federal grant programming in homeland and civil security (with a focus on critical infrastructure protection), the following steps should be considered:

- Increase state and local ownership in federal programs and national security problems;
- Address interaction of infrastructure and (political, civic, organizational, and security) culture more strongly and consistently; and
- Emphasize the value-added (or subsidiary) character of federal programs with regard to state and local initiatives.

Andrea Jerkovic may be reached at jerkovic@european-security.info

The Light Under the Bushel — Redefining US National Security by Leveraging Principles of Human Security to Address Underlying Causes of Asymmetric Insurgencies

by Dr. Elisabeth Hope Murray, Embry-Riddle Aeronautical University
& Dr. Jim Ramsay, University of New Hampshire

UAPI and Naval Postgraduate School Center for Homeland Defense and Security
10th Anniversary Summit, George Mason Arlington Campus, 2017

The primary purposes of the American institutions of governance are to secure and protect the citizens of the state; the belief that our government has the will and ability to do so is one of the reasons citizens continue to believe in the greatness of America. However, current US national security strategies have struggled to protect individuals from the social, economic, and political chaos incited by the emergence of transnational (asymmetric) challenges such as terrorism and other macro-regional threats such as climate change. If our government is intent on preventing the development of the next radical group, such as Al-Qaeda, Al-Shabaab, or ISIS, the national security dialogue, and consequently the next strategy, must directly and intentionally incorporate principles of human security. Most insurgent groups have definitive, foundational links to human security crises: food insecurity, water insecurity, increasing fragile livelihoods, inadequate access to economic burden sharing, and limited resource availability. The US is the global leader in military humanitarian relief and is the only military in the world that has formalized global relief efforts through a separate office: the office of Overseas Humanitarian, Disaster and Civic Aid (OHDACA). OHDACA receives a separate annual budget allocation for three thematic windows: humanitarian mine action, humanitarian assistance, and foreign disaster relief, critical at a time where, from 2001 to 2011, the annual average number of people affected by natural disasters has risen by 232%, compared to 1990 to 2000. Similarly, increased attention is being paid in the US Military to the cost-benefit of policies supporting the prevention and mitigation of social and ideological radicalization. We propose that human security principles be integrated more formally into the US national security strategy.

In light of the challenges posed by climate change and the lesser, but still crucial challenges posed by asymmetrical terrorism, we say with certainty that now more than ever before we need the full integration of a human security paradigm to emerge in tandem with the current

national security sector present in American policy making. Strategic plans specifically identifying the non-linear nature of wicked threats need to be initiated as soon as possible in order to begin limiting the power of these threats on American security specifically and human security more generally. We believe the Department of Homeland Security to be in a unique position to provide the leadership and structure to institute such critical changes. With its dual focus on Emergency Management and Counter-terrorism, the foundational ideological and practical structures are already in place. These structures are critical, as without a structured, strategic approach to wicked security threats, a new American human security paradigm will fail. Our paper details specific areas where a greater focus on human security could relate directly to the increased security of the US state and its citizens.

Lead author Elizabeth Hope Murray may be reached at murraye4@erau.edu

Improving Citizen Threat Preparedness & Recovery

by Robert Mandel

Within the homeland security context, this paper examines obstacles to effective mass participation, ways to enhance citizen accountability and vigilance in the face of threat, and value controversies embedded in this thrust. The goal is to expand and refine existing techniques so as to improve citizen preparation and recovery regarding ominous human security dangers. Although the quest to improve mass public involvement in its protection from internal and external threat is not new, there is considerable room for improvement.

The principal obstacles to citizen threat preparedness and recovery are paralyzing citizen fears, citizen protection measurement difficulties, and citizen safety misperceptions. The ways to enhance citizen accountability and vigilance in the face of threat include wider adoption of a two-pronged top-down/bottom-up approach that directly involves both government and society; more integrated coordination is needed among relevant private and public players in the citizen protection game, improving incentives for cooperation and resolving public-private differences; and expanded citizens' accountability, preparedness, and vigilance needed to increase (1) their post-disruption resiliency, (2) their government input quality, and (3) their personal safety measures. The value controversies embedded in this thrust include finding ways to restore mutual state-society trust, to minimize tradeoffs between human security and state security, to raise the priority of public safety concerns, and to promote stabilizing civil society norms. While these recommendations may seem familiar, new ways of pursuing these objectives (suggested in the paper) can improve both their effectiveness and legitimacy.

In reflecting on the relative importance of citizen protection, a dual danger exists of either overreacting or underreacting to homeland security threats. The greatest challenge remains prioritizing properly what is most important to state and society. The path to secure citizen protection entails considerable subtlety and sensitivity about diverse threats and responses, depending on security vulnerabilities, threat tolerance, compromise possibilities, risk propensities, physical and psychological resiliency, and value aspirations. To improve threat responses, security officials need more creative, innovative, outside-the-box thinking. Delusions, misperceptions, miscommunications, inconsistent actions, and confounding paralysis about homeland security could be tolerable if the world's citizens were universally experiencing robust safety, but such is not the case.

There is no viable alternative to beginning now to take concrete steps to improve citizen threat preparedness and recovery. Despite extensive efforts in this direction since 9/11, we can certainly do better. The individual security impact of anarchic violence on unhealthy lifestyles, personal damage vulnerability, civil society norm erosion, and lawlessness could, if left unchecked, so remove any sense of order that government would ultimately be utterly unable to function. We citizens must get the ball rolling to advance our security by undertaking better monitoring of genuine dangers and vigilance about state threat responses, faster means to return to normal after shocks, and more effective independent state-coordinated initiatives to maximize our own safety. The author may be reached at mandel@lclark.edu.

Apples-to-Apples: LIRA vs. RAMCAP

by Randy George, Rick White, C. Edward Chow, and Terrance Boulton

In October 2014, the Department of Homeland Security Science and Technology Directorate (DHSS&T) contracted the University of Colorado, Colorado Springs (UCCS) to evaluate RAMCAP, the Risk Analysis and Management for Critical Asset Protection. RAMCAP was developed by the American Society of Mechanical Engineers (ASME) at the request of the White House shortly after 9/11 to uniformly assess risk and help prioritize national investments in critical infrastructure protection. Despite four years working with stakeholders, RAMCAP was rejected after it was introduced in the 2006 National Infrastructure Protection Plan. Among its few surviving applications, RAMCAP is designated the J100-10 standard for risk analysis on Water and Wastewater treatment plants. It was for this reason that DHS returned to RAMCAP in 2014 over concerns for the nation's deteriorating drinking water infrastructure.

In the United States, about 156,000 public water systems provide drinking water to about 320 million people through more than 700,000 miles of pipes. Unfortunately, much of the system is starting to come to the end of its useful life, with many of the pipes over 100 years old. As a consequence, there are an estimated 240,000 water main breaks per year contributing to the estimated 1.7 trillion gallons of water lost to broken and leaky pipes. The cost to fix the system is estimated somewhere between \$650 billion and \$1 trillion.¹ Most water utilities are unprepared to take on this expense. The Environmental Protection Agency (EPA) doesn't have the money,² nor does Congress, having allocated only \$17.3 billion to the Drinking Water State Revolving Fund (DWSRF) over the past 20 years;³ [3] less than 3% needed to fix the problem based on the lowest estimate.

Leaky pipes are not the only concern. Climate change also poses a threat to the nation's drinking water infrastructure. Higher air and water temperatures promote increased growth of algae and microbes, increasing the need for drinking water treatment. Higher air and water temperatures also melt the polar ice caps causing global sea levels to rise. Sea-level rise increases the salinity of both surface and ground water, resulting in salt-water intrusion into coastal drinking water supplies. Reduced annual precipitation and extended drought threaten in-land water supplies. Climate change presents yet another challenge for which utilities are unprepared to pay the bill.⁴

1 M. Morrow, "America's Water Infrastructure Is in Need of a Major Overhaul," FOX Business, 28 January 2016. [Online]. Available: <http://www.foxbusiness.com/features/2016/01/28/america-s-water-infrastructure-is-in-need-major-overhaul.html#>. [Accessed 6 February 2016].

2 US Environmental Protection Agency, "EPA Response to EO 13636, Improving Critical Infrastructure Cybersecurity," Washington, DC, 2014.

3 U.S. Environmental Protection Agency, "How the Drinking Water State Revolving Fund Works," [Online]. Available: <http://www.epa.gov/drinkingwatersrf/how-drinking-water-state-revolving-fund-works#tab-1>. [Accessed 6 February 2016].

4 U.S. Environmental Protection Agency, "Climate Change Adaptation Plan," Washington, DC, 2014.

As if these concerns aren't enough, water utilities also face the threat of terrorist attack. 9/11 demonstrated the ability of small groups to inflict catastrophic destruction by subverting critical infrastructure. Water utilities are not just critical, they are considered a "lifeline" function; they are essential to the operation of most other critical infrastructure sectors. Water utilities are considered "lifeline" functions together with communications, transportation, and energy. Moreover, water utilities pose a potential target because about 15% of facilities provide services to more than 75% of the US population.⁵ A carefully executed cyber attack could conceivably disrupt the distribution systems for these supplies.

Concerned about these emerging threats to the nation's drinking water from aging infrastructure, climate change, and cyber attack, in 2014 DHS S&T launched the Drinking Water Resilience Project (DWRP). Whenever faced with more tasks than resources, one must prioritize. DWRP sought an objective risk methodology to help prioritize national investments, not just in water utilities, but all lifeline infrastructures. DHS S&T tasked UCCS to evaluate RAMCAP for this capability.

Detailed analysis involving modeling and simulation determined that RAMCAP did not account for emerging threats from aging infrastructure, climate change, or cyber attack. Nor could RAMCAP account for mobile assets, leaving out the entire aviation subsector. Most significantly, RAMCAP allowed wide variability in its calculations, making the results incomparable across assets or sectors. Overcoming these shortfalls would require a major overhaul of RAMCAP. The first step was expanding RAMCAP's reference scenarios to include the emerging threat categories. The second step was more drastic. To accommodate mobile assets, RAMCAP's bottom-up component analysis had to be replaced with a top-down system analysis. And perhaps the greatest challenge, the third step was to outfit RAMCAP with a default database of threat and vulnerability values to eliminate variability so risk results could be compared "apples-to-apples". To demonstrate the feasibility of these changes, UCCS developed a prototype model called LIRA for Lifeline Infrastructure Risk Analysis.

LIRA met the objectives set by DWRP. DHS S&T wanted to submit it for certification by the American National Standards Institute (ANSI), and help LIRA avoid the fate of RAMCAP. DHS S&T thus contracted UCCS a second year in October 2015 to develop the corresponding ANSI-standard specification. As part of the process, UCCS was tasked to incorporate stakeholder feedback on the LIRA design. This was done through an online survey administered between February and May 2016.

The LIRA survey was comprised of ten "Would you rather..." questions. The questions were formulated to gauge user preferences between fundamental differences in LIRA and RAMCAP designs. LIRA trades detailed results for speed and cost savings. RAMCAP trades speed and cost savings for detailed results. At the conclusion of the survey, participants expressed an overwhelming preference for LIRA. Unfortunately, the results were convincing, but not conclusive. Despite reaching out to 684 representatives from the aviation, electricity, and drinking water subsectors, only 26 people responded to the survey. The confidence intervals were too large to make the results definitive. Before making a substantial investment in ANSI certification, DHS S&T wanted to confirm the results. Consequently, UCCS was contracted a third year in October 2016 to repeat the survey and also deliver a tool to help build the LIRA database.

5 U.S. Department of Homeland Security, "National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience," US Department of Homeland Security, Washington, DC, 2013.

Epilogue. Since this paper was submitted, UCCS completed its obligations under the DWRP Y3 contract. The survey was again under-represented, garnering only 49 more responses. This time, though, the results were mixed, favoring neither RAMCAP nor LIRA. The confusion may be attributable to a design flaw in the survey. It doesn't matter. In August 2017, UCCS released the LIRA Database Validation Tool. LIRA-DVT is a complete online implementation of the LIRA risk methodology including a default data set. The purpose of LIRA-DVT is to collect locally-adjusted changes to the default database. The collected data is anonymous, and cannot be traced back to the user. A LIRA risk analysis can take less than thirty minutes. In addition to providing an objective assessment of risk at the local, state, and national levels, LIRA also helps users examine the cost benefits of alternative mitigation and resilience measures. LIRA-DVT is available for free at <https://lira.uccs.edu/app/>. Rick White may be reached at rwhite2@uccs.edu

Online Human Behaviors on Social Media During Disaster Responses

by JooHo Kim and Makarand Hastak

Executive summary

Social media plays a critical role in natural disasters as an information propagator that can be leveraged for disaster responses. This study analyzed the online user engagement on social media during the 2016 Louisiana Flood through the lens of Social Network Analysis (SNA). Our findings revealed temporal and spatial characteristics of online social engagement as well as a trend of online users' interests during the flood. We also identified how social capital/infrastructure and community leaders were engaged in improving a flood inundation map. The results will assist emergency agencies and organizations to understand characteristics of social media and the user behaviors during disasters.

Introduction

Social media platforms, such as Twitter and Facebook, play a vital role in disaster management by propagating emergency information to a disaster-affected community. Social media ranks as the fourth most popular source for accessing emergency information. Thus, emergency agencies need to understand characteristics of online social engagement and the network structure created by online user communications to expedite emergency information diffusion via their social media. The 2016 flood in Louisiana damaged more than 60,000 homes and was the worst U.S. disaster after Hurricane Sandy in 2012. The no-name storm deposited about 7.1 trillion gallons of water on Louisiana comparing to Hurricane Katrina (2.3 trillion gallons) and Hurricane Isaac (5.3 trillion gallons). The major media has been criticized by many leaders in Louisiana for the lack of coverage of the 2016 Louisiana flood, especially compared to the other major natural disasters in the U.S. (Berman, 2016; May & Bowerman, 2016; Pallotta, 2016; Scott, 2016). During the period, the media mainly covered the 2016 U.S. presidential election and the 2016 Rio Summer Olympics. Craig Fugate, the administrator of the FEMA, stated: "You have Olympics, you got the election. If you look at the national news, you are probably on the third or fourth page. ... We think it is a national headline disaster" (O'Donoghue, 2016). Parishes in Louisiana actively used their social media such as Twitter and Facebook to share information with the disaster-affected community – e.g., flood inundation map, locations of emergency shelters, medical services, and debris removal operation. This study investigated online user behaviors on Facebook in the city of Baton Rouge (CBR) during the 2016 Louisiana flood. We collected data from the Facebook page ([facebook.com/cityofbatonrouge](https://www.facebook.com/cityofbatonrouge)) during August 12 – December 1, 2016.

Results

The CBR used both Twitter and Facebook to share emergency information. The number of engagement on Facebook was higher than Twitter during the flood. The trend of Facebook engagement significantly increased in the first two weeks, reached its peak on August 20, and then declined over time: 47% of the engagements were generated within the first two weeks. We measured online user centrality to determine the prominence or importance of users in the network. The degree distributions are very heterogeneous and highly right-skewed (Kim & Hastak, 2018). That is, there were certain hubs in the network. The results revealed that individuals and agencies/organizations have different roles in the network. The individual users actively shared emergency information with their online friends by multiple activities such as tagging their friends, posting a comment, or sharing information with their online community: (1) like (76.56%), (2) comment (15.55%) and (3) share a (7.99%). In contrast, organizations/agencies played a critical role in connecting a network of the city of Baton Rouge with external social groups or online communities as a gatekeeper. Overall, the core of the online community consisted of numerous individuals, while agencies and organizations linked other communities.

Conclusions/Discussions

We compared search-term trends about the 2016 Louisiana flood and Hurricane Sandy of 2012. There were summer Olympic Games and presidential elections around the time of both disasters, but the trends of online user interests were significantly different. People's interest in the 2016 Louisiana flood was not significant and was lower than that shown for the summer Olympic Games and the presidential election, even though it was recorded as the worst disaster after Hurricane Sandy. Further investigations are needed to answer how these national events affect emergency information diffusion via social media and user behaviors during disaster responses.

We compared social engagement on Twitter and Facebook operated by CBR. Contrary to literature, disaster-related information was diffused actively via Facebook rather than Twitter during the flood (as of Oct 3 2018, 10,748 followers on Facebook and 16,500 followers on Twitter). There might be several reasons behind this. Firstly, Facebook has multiple functions for sharing numerous types of messages including images, videos, and hyperlinks. This flexibility of the platform might help users understand information faster and trigger them to share the information with others. Also, frequency of social media use might affect the difference of online engagement on Twitter and Facebook. Duggan (2015) identified that of Facebook's total number of users, 70% visit the platform daily, while for Twitter this is 38%. Thus, more people might have a chance of being engaged in emergency information via Facebook.

Recently, Twitter doubled the text limit from 140 to 280 characters (Issac, 2017). It might affect Twitter user behaviors and patterns during disaster responses.

It is critical for the public to receive accurate, reliable and timely information from emergency agencies during disasters. As our findings reveal, SNA can be used to understand the heterogeneity of a large-scale social network and applied to accelerate information diffusion in emergency. A structure of social network would be homogeneous, but the components

(vertices and edges) would be heterogeneous based on the built environment and human behaviors in a community. Thus, emergency agencies keep monitoring online social behaviors and engagement during multiple disasters and understand their characteristics in local-, state- and national level. Most questions could be answered by a multi-case study approach that would compare the use and effectiveness of social media across a broad range of disasters.

About the Authors

Joocho Kim Ph.D. candidate, Division of Construction Engineering and Management, Purdue University, 550 Stadium Mall Dr., West Lafayette, IN 47907, USA. E-mail: joohoya@gmail.com

Makarand Hastak Professor and Head, Division of Construction Engineering and Management; Professor of Civil Engineering, Purdue University, 550 Stadium Mall Dr., West Lafayette, IN 47907, USA. E-mail: hastak@purdue.edu

References

Berman, R. (2016). America is ignoring another natural disaster near the Gulf. Retrieved January 16, 2017, from <http://www.theatlantic.com/politics/archive/2016/08/america-is-ignoring-another-natural-disaster-near-the-gulf/496355/>

Duggan, M. (2015). The Demographics of Social Media Users. Retrieved December 17, 2016, from <http://www.pewinternet.org/2015/08/19/the-demographics-of-social-media-users/>

Hersher, R. (2016). Flooding In Louisiana Raises Questions About Timing, Urgency Of Warnings. Retrieved March 1, 2017, from <http://www.npr.org/sections/thetwo-way/2016/08/22/490916070/flooding-in-louisiana-raises-questions-about-timing-urgency-of-warnings>

Issac, M. (2017). Twitter to Test Doubling Tweet Length to 280 Characters – The New York Times. Retrieved September 27, 2017, from <https://www.nytimes.com/2017/09/26/technology/twitter-280-characters.html?mcubz=1>

Kim, J., & Hastak, M. (2018). Social network analysis: Characteristics of online social networks after a disaster. *International Journal of Information Management*, 38(1), 86–96. <https://doi.org/10.1016/j.ijinfomgt.2017.08.003>

May, A., & Bowerman, M. (2016). Louisiana flooding is worst disaster since Sandy, but people aren't talking about it. Retrieved January 16, 2017, from <http://www.usatoday.com/story/news/nation-now/2016/08/18/louisiana-flooding-worst-disaster-since-sandy-but-people-arent-talking/88942460/>

O'Donoghue, J. (2016). Louisiana Flood of 2016: 15 things you need to know on Tuesday. Retrieved March 1, 2017, from http://www.nola.com/weather/index.ssf/2016/08/louisiana_flooding.html#incart_big-photo

Pallotta, F. (2016). National media criticized over Louisiana flooding coverage – Aug. 18, 2016. Retrieved January 17, 2017, from <http://money.cnn.com/2016/08/18/media/louisiana-flooding-media-coverage/>

Scott, M. (2016). National media fiddle as Louisiana drowns | NOLA.com. Retrieved January 16, 2017, from http://www.nola.com/weather/index.ssf/2016/08/national_media_louisiana_flood.html

Social Times. (2016). Here's How Many People Are on Facebook, Instagram, Twitter and Other Big Social Networks. Retrieved December 17, 2016, from <http://www.adweek.com/socialtimes/heres-how-many-people-are-on-facebook-instagram-twitter-other-big-social-networks/637205>

Defensibility and Risk Management

Vicki Bier, Alexander Gutfraind, and Ziyang Lu

A common problem in risk management is to characterize the overall security of a system of valuable assets (e.g., government buildings or communication hubs), and to suggest measures to mitigate any security threats. Currently, analysts rely on a combination of security indices, such as resilience (the ability of a system to return to normal rapidly); robustness (the ability to function despite damage); redundancy (spare capacity); security (barriers to limit access); and vulnerability (susceptibility to hazards and/or intentional threats). However, these indices are not always actionable; i.e., they are not themselves sufficient to indicate whether policy makers should invest in improving a given system. Indeed, it has been observed that some vulnerable systems cannot be improved cost-effectively [1].

Motivated by this gap, we recently proposed an index, defensibility [2], which characterizes how easily the damage to a system can be reduced. A system is highly defensible if a modest investment of resources can significantly reduce the damage from an attack or disruption (Fig. 1). Defensibility is defined in such a way that incommensurable systems can be compared to each other using a single measure. The most defensible system would then receive the highest priority for defensive resources.

We compute the measure outlined above for several representative data sets, including property losses data from Willis [3] and air transportation data from the US Department of Transportation. We also derive rigorous results for an important class of problems involving discrete assets of differing values, such as airports, military bases, or commercial buildings. Among our more surprising findings is that some types of systems may be more defensible against deliberate attackers than against random hazards.

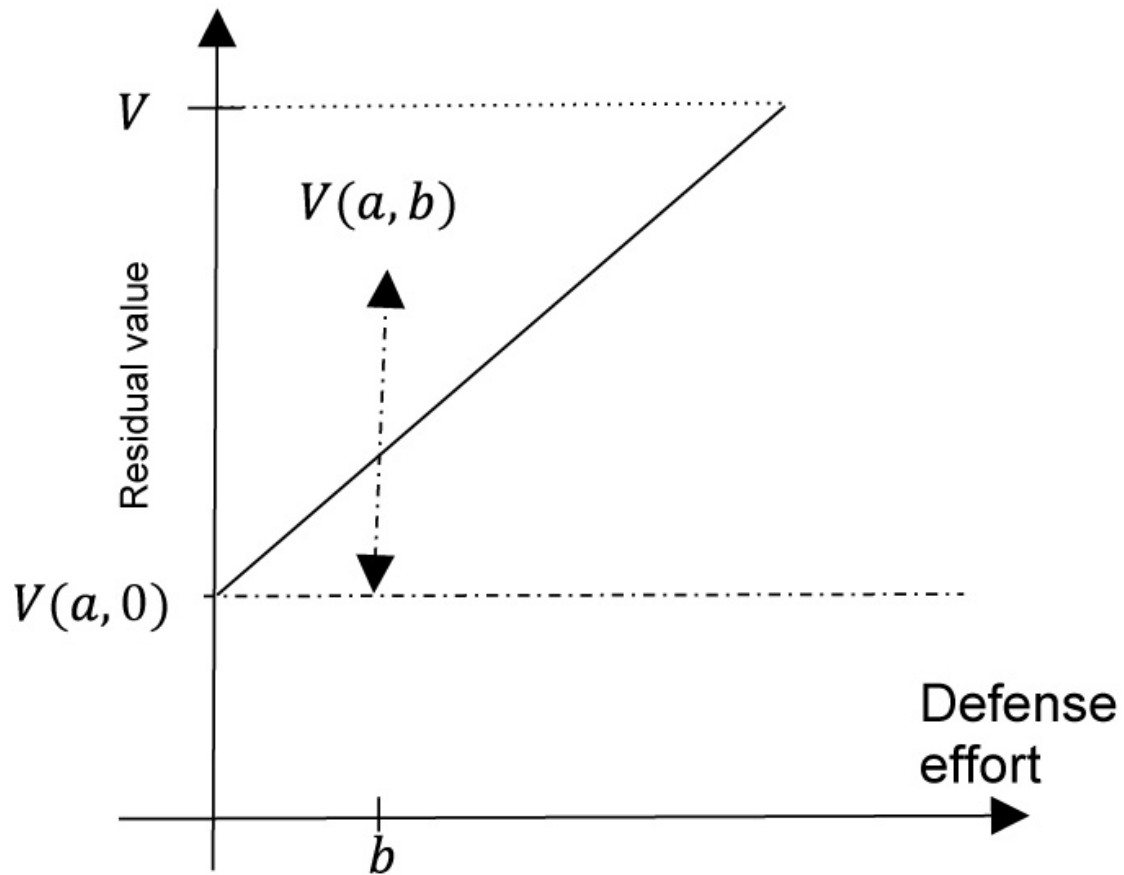


Fig. 1. Hypothetical curves showing the residual values of three systems with different defensibilities. $V(a, 0)$ and $V(a, b)$ are, respectively, the residual values of the system after an attack effort a in the case of zero defense effort and effort b , respectively. The upper (concave) curve represents a highly defensible system, where a small defense effort results in a large increase in the residual value of the system. Its defensibility at the point b is indicated by the vertical arrow between the upper curve $V(a, b)$ and the dashed line $V(a, 0)$.

To summarize, security analysis to date has been focused on existing notions such as vulnerability and resilience. Our analysis here is based on the observation that some at-risk systems may be much easier to improve than others. We argue that risk analysts and managers would benefit by considering defensibility in their risk management plans.

About the Authors

Prof. Vicki Bier, PhD. Department of Industrial and Systems Engineering, University of Wisconsin-Madison, 1513 University Avenue, Madison, WI, 53706 USA bier@engr.wisc.edu

Prof. Alexander Gutfraind, PhD. Uptake Technologies, Inc, 60654, Chicago, IL and Laboratory for Mathematical Analysis of Complexity and Conflicts Loyola University Medical Center, Maywood, IL, 60153 USA agutfraind.research@gmail.com

Mr. Ziyang Lu. Department of Industrial and Systems Engineering, University of Wisconsin-Madison, 1513 University Avenue, Madison, WI, 53706 USA zlu55@wisc.edu

Bibliography

- [1] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, and K. R. Wierzbicki, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 9, pp. 1155–1161, Sep. 2007.
- [2] V. M. Bier and A. Gutfraind, "Risk analysis beyond vulnerability and resilience – characterizing the defensibility of systems and targets," *Risk Anal.*, under revision 2017.
- [3] H. H. Willis, "Guiding Resource Allocations Based on Terrorism Risk," *Risk Anal.*, vol. 27, no. 3, pp. 597–606, Jun. 2007.

