NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BEYOND THE FIRST 48:
INCORPORATING NONTRADITIONAL STAKEHOLDERS INTO INCIDENT RESPONSE

by

Emily J. McLoughlin

September 2020

Thesis Advisor: Shannon A. Brown
Second Reader: John Rollins,
NPS Center for Homeland Defense and Security

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2020	3. REPORT TYPE AND DATES COVERED Master's thesis

4. TITLE AND SUBTITLE
BEYOND THE FIRST 48: INCORPORATING NONTRADITIONAL STAKEHOLDERS INTO INCIDENT RESPONSE

5. FUNDING NUMBERS

6. AUTHOR(S) Emily J. McLoughlin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

During a catastrophic attack or cyber-attack on critical infrastructure, how can local emergency management agencies integrate nontraditional stakeholders successfully into incident response operations? A wide variety of stakeholders who are not traditionally involved in incident response will likely be critical at this time—such as human services, the transportation sector, and private-sector entities. This thesis first explores an academic discussion of the current incident response framework, comprising the National Incident Management System (NIMS) and the Incident Command System (ICS). The thesis then uses a scenario based around a large-scale water outage to illustrate the potential cascading impacts and gaps of the status quo framework. The research shows that NIMS and ICS do not effectively incorporate nontraditional stakeholders into incident response operations at the local government level, and that this framework should be reserved for traditional first responders working to stabilize life safety at an incident scene. This study highlights capabilities that local governments should focus on to ensure their organizational readiness to respond to a critical infrastructure outage that may have catastrophic impacts.

14. SUBJECT TERMS
non-traditional stakeholders, private sector, critical infrastructure, emergency management, first responder, National Incident Management System, Federal Emergency Management Agency, local government, state government

15. NUMBER OF PAGES
111

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

BEYOND THE FIRST 48: INCORPORATING NONTRADITIONAL STAKEHOLDERS INTO INCIDENT RESPONSE

Emily J. McLoughlin

Program Manager, Emergency Preparedness, Department of Public Safety Communications and Emergency Management, Arlington County Government
B, Hobart and William Smith Colleges, 2009
MPA, George Mason University, 2015

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
September 2020

Approved by: Shannon A. Brown
Advisor

John Rollins
Second Reader

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

During a catastrophic attack or cyber-attack on critical infrastructure, how can local emergency management agencies integrate nontraditional stakeholders successfully into incident response operations? A wide variety of stakeholders who are not traditionally involved in incident response will likely be critical at this time—such as human services, the transportation sector, and private-sector entities. This thesis first explores an academic discussion of the current incident response framework, comprising the National Incident Management System (NIMS) and the Incident Command System (ICS). The thesis then uses a scenario based around a large-scale water outage to illustrate the potential cascading impacts and gaps of the status quo framework. The research shows that NIMS and ICS do not effectively incorporate nontraditional stakeholders into incident response operations at the local government level, and that this framework should be reserved for traditional first responders working to stabilize life safety at an incident scene. This study highlights capabilities that local governments should focus on to ensure their organizational readiness to respond to a critical infrastructure outage that may have catastrophic impacts.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
- A. EMERGING THREATS AND GAPS IN RESPONSE CAPABILITIES 1
- B. RESEARCH QUESTION 3
- C. DEFINING THE PROBLEM SPACE: THE SOTHIRSTY SCENARIO 3
- D. DEFINITIONS 6
- E. METHODOLOGY 7

II. UNTAPPED RESOURCES: THE INCIDENT RESPONSE SYSTEM AND NONTRADITIONAL STAKEHOLDERS 11
- A. WICKED PROBLEMS 13
- B. WAR GAMING AS A TOOL FOR REAL PREPAREDNESS 16
- C. THE APPLICATION OF ICS TO CATASTROPHIC INCIDENTS 19
- D. ICS AS A NETWORK RATHER THAN A HIERARCHY 21
- E. PRACTICAL CHALLENGES TO THE IMPLEMENTATION OF NIMS AND ICS 23
- F. CONCLUSION 25

III. OUT WITH THE OLD, IN WITH THE NEW: TRANSITIONING AWAY FROM ICS 27
- A. NIMS AND ICS: IMPERFECT SYSTEMS 30
- B. EXPANDING THE UNDERSTANDING OF THE RESPONSE PHASE 33
- C. CONCLUSION 37

IV. COMPONENTS FOR A NEW APPROACH 39
- A. FIVE CAPABILITIES 42
  - 1. An Established, Comprehensive Common Operating Picture through Information Sharing 42
  - 2. The Right People at the Table 44
  - 3. Government's Ability to Do Business with the Private Sector 45
  - 4. Easy-to-Understand Information-Sharing Practices 46
  - 5. Regional Coordination and Communication 51
- B. CONCLUSION 52

V. CONCLUSION: DIRECTION FOR STRUCTURAL CHANGE 53
A. FINDINGS 54
B. CONCLUSIONS 55
C. RECOMMENDATIONS FOR STRUCTURAL CHANGE 57
1. Establish Emergency Management as a Field Independent of First Responders 57
2. Authorize Local Governments to Develop EOC Policies and Procedures Specific to Their Needs 58
3. Prioritize Local Government's Incorporation of the Private Sector in All Phases of Emergency Management 59
D. FUTURE RESEARCH 60
E. POSTSCRIPT 60

APPENDIX A. SOTHIRSTY TABLETOP EXERCISE 63

APPENDIX B. COMPILED SOTHIRSTY SCENARIO 75
A. SCENARIO MOVE 0 76
B. SCENARIO MOVE 1 77
C. SCENARIO MOVE 2 80
D. SCENARIO MOVE 3 83

LIST OF REFERENCES 85

INITIAL DISTRIBUTION LIST 91

LIST OF FIGURES

Figure 1. SoThirsty Scenario Move 0 (00:01–00:30 Minutes) 5

Figure 2. SoThirsty Scenario Move 1 (00:30–24:00 Hours).....11

Figure 3. Worst-Case Impacts: SoThirsty Scenario Move 1.....12

Figure 4. Best-Case Impacts: SoThirsty Scenario Move 1 13

Figure 5. SoThirsty Scenario Move 2 (72:00 Hours).....27

Figure 6. Worst-Case Impacts: SoThirsty Scenario Move 2.....28

Figure 7. Best-Case Impacts: SoThirsty Scenario Move 2 29

Figure 8. Response Phase Subsections.....34

Figure 9. SoThirsty Scenario Move 3 (Day 7) 39

Figure 10. Worst-Case Impacts: SoThirsty Scenario Move 3.....40

Figure 11. Best-Case Impacts: SoThirsty Scenario Move 3 40

Figure 12. NIMS Planning “P”.....48

Figure 13. Amended Planning “P” 50

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BEOC	business emergency operations centers
COP	common operating picture
EOC	emergency operations center
FEMA	Federal Emergency Management Agency
FIRESCOPE	Firefighting Resources of Southern California Organized for Potential Emergencies
HSEEP	Homeland Security Exercise and Evaluation Program
ICS	Incident Command System
NIMS	National Incident Management System

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Cyber-attacks will create grave homeland security consequences in the coming years: power outages that last for weeks, drinking water supplies tainted with bacteria, and other destructive outcomes that are likely to result in the loss of human life and the destruction of property. At the local government level, a wide variety of stakeholders not traditionally involved in incident response—such as human services, the transportation sector, and private-sector entities—will be critical to response operations during these incidents. The central problem addressed in this thesis is how to integrate these stakeholders successfully in incident response operations that occur at an emergency operations center (EOC). Because of the introduction of new stakeholders and the complicated nature of cyber-attacks, a divergence from the National Incident Management System (NIMS) and the Incident Command System (ICS) is required for local EOCs to best manage incident response operations.

Despite national implementation, NIMS and ICS are not suited for incident response operations that occur at the local government level, that rely on nontraditional responders, and that occur in an EOC. This is partially because NIMS and ICS were originally created to support of the California fire service; the hierarchical approach appropriate for managing a large-scale event with homogenous responders, like a wildfire, does not work when nontraditional stakeholders are needed. Essentially, NIMS and ICS are intended for field operations rather than for EOC functionality.

To illustrate the limitations of NIMS and ICS, this thesis develops a scenario called SoThirsty to depict the potential cascading impacts of a catastrophic water outage in the National Capitol Region. The scenario features rich details that illustrate the drawbacks of NIMS and ICS as a response framework for a novel critical infrastructure outage that relies heavily on nontraditional stakeholders, and where incident response operations are managed from an EOC. As the SoThirsty scenario illustrates, nontraditional stakeholders are integral to response operations in this type of event due to their relevant subject matter expertise, and traditional first responders have a diminished role. Because of the systemic

challenges with incorporating nontraditional stakeholders into incident response operations, agencies must examine and improve the existing response framework.

Based on analysis of the SoThirsty scenario, this thesis highlights five capabilities that local governments must adopt to successfully manage incident response operations to a catastrophic incident that does not rely primarily on traditional first responders. These five capabilities serve as guiding lights for local jurisdictions to create their own alternative incident response infrastructures. Rather than sticking to a rigid, one-size-fits-all structure like NIMS and ICS, local governments should be able to coordinate response operations in a manner that works best for them and all of their stakeholders. The focus should be on adaptability, and on an approach that is complementary to a jurisdiction's organizational structure and the needs of private-sector organizations that can bring critical resources to the table. The five capabilities are:

- *An established, comprehensive common operating picture through information sharing*: Jurisdictions must develop infrastructure capable of gathering information to feed into a common operating picture from a wide range of sources.

- *The right people at the table*: Representatives in the EOC must have a tactical understanding of their organization's capabilities and the authorization to make decisions about resource allocation.

- *Government's ability to do business with the private sector*: Government entities must establish protocols prior to an emergency incident that facilitate resource sharing and procurement of goods from the private sector.

- *Easy-to-Understand Information-Sharing Practices*: Common-sense terminology and concepts must be used to convey the organizational structure and responsibilities of each representative in an EOC.

- *Regional coordination and communication*: Inter-jurisdictional communication and coordination is a critical element of incident response operations, regardless of jurisdictional EOC structures.

Jurisdictions across the country will need to engage in collaborative work to identify the practices and policies that work best for them.

As a relatively young professional field, emergency management has reached a major crisis of character. Are emergency managers first responders or not? Because the emergency management profession has aligned itself so closely with first responders, it has decreased opportunities for collaboration with other critical stakeholders. As the nation faces new threats and hazards, like those from a catastrophic attack against critical infrastructure, counties' strategic postures must be reevaluated. As emergency managers consider new threats and hazards, it is critical for them to grow the spectrum of potential partners in incident response.

The thesis concludes with three recommendations that serve as a road map for how local governments can implement an alternate incident response framework for catastrophic critical infrastructure outages. First, emergency management must be established as a field independent from first responders. Until the difference between emergency managers and first responders is recognized enterprise-wide, the incorporation of nontraditional stakeholders in incident response will stall, leaving precious critical resources unutilized during a crisis. An incident response framework that can only be understood by one group of stakeholders reflects a lack of imagination around the types of threats and hazards the nation is facing today.

Second, local governments must be authorized to develop EOC policies and procedures specific to their needs. It is likely that EOCs are already unofficially adapting NIMS and ICS. Every local government EOC that does not have the personnel to fully staff ICS, or abandons the Planning "P," provides an example of where the formal structures are being reworked to suit resource constraints and better judgement.

Finally, local governments must prioritize the incorporation of the private sector in all phases of emergency management. The value of developing a preparedness curriculum

for the private sector is twofold. First, when businesses are prepared for a crisis, they free up critical government resources and can contribute to response efforts rather than draw down limited resources. And second, outreach efforts to engage the private sector start a dialogue about emergency management's mission space, how the private sector may be called on, and how they can best help. Ultimately, the private sector must be as engaged as every traditional emergency management partner.

ACKNOWLEDGMENTS

My successful completion of the Center for Homeland Defense and Security's master's program is the result of support from a wide range of sources. The following notes are an attempt to thank those whose support is most memorable at the time of writing, but this is by no means an exhaustive list.

To my 1801/1802 cohort classmates: without them, I would not have made it through this program. Their humor, encouragement, and enthusiasm about my thesis topic propelled me through this process and gave me the drive I needed to reach the finish line.

To my advisor, Dr. Shannon Brown, for sticking with me through the evolution of this thesis and for taking a chance on an unusual style. Our collaboration has been one of the highlights of my time in this program. Additionally, I would like to thank my second reader, John Rollins, who did not back down when pushing me to do my best work.

To the entire Department of Public Safety Communications and Emergency Management in Arlington County, Virginia, for their support and patience with me over the past eighteen months.

To William N. Flagler Jr., who has given me the gift of education, one of the greatest you can be given. I could not have completed this program without his support. He has always seen the best in me and that made all the difference.

And finally, to my dear husband, who supported me day and night. His patience, compassion, and humor carried me through this journey—one that has tested me in every way—and forced him to learn more than he ever wanted to know about homeland security.

In Memory of
Lieutenant Steven Acton
District of Columbia Fire and EMS Department
April 22, 1984–July 30, 2018

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Prior to 9/11, CIA Director George Tenet pronounced that the warning lights of an impending terrorist attack were "blinking red."[1] However, the nation's intelligence agencies and systems could not discern the nature of the novel attack in a way that allowed them to issue an actionable warning. In 2018, the director of national intelligence, Dan Coates, established that "the warning lights are blinking red again," this time for an impending cyber-attack.[2]

The nation's risk profile has expanded due to our continuous dependence on industrial and information technology systems for stability in critical infrastructure operations. Any system that connects to the internet is susceptible to a cyber-attack and seizure by a malicious actor. Loss of control of critical infrastructure systems will have a severe impact on day-to-day life and disrupt the American quality of life in the long term.

A. EMERGING THREATS AND GAPS IN RESPONSE CAPABILITIES

Cyber-attacks can create grave homeland security consequences: power outages that last for weeks, drinking-water supplies tainted with bacteria, and other destructive outcomes that will lead to the loss of human life and destruction of property. A catastrophic cyber-attack on critical infrastructure will exceed local government's resource and response capabilities; partners from other government departments and the private sector will need to be quickly incorporated. A wide variety of stakeholders not traditionally involved in incident response, such as human services, the transportation sector, and private-sector entities, will be critical to response operations. The central problem addressed in this thesis deals with how to integrate these stakeholders successfully into incident response operations.

---

[1] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (Washington, DC: Government Printing Office, 2004), 259, https://www.9-11commission.gov/report/.

[2] Julian Barnes, "Warning Lights Are Blinking Red," *New York Times*, July 13, 2018, https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

Nationally, the organization of emergency incident response falls under the National Incident Management System (NIMS), which is built around the Incident Command System (ICS) subcomponent. A central criticism of these structures is their inability to incorporate nontraditional stakeholders, which inhibits their effectiveness during incidents that do not primarily rely on first responders.[3] While a purported core feature of NIMS and ICS is their use of easy-to-understand terms and concepts, extensive academic and practical discussion show otherwise. For example, during a crisis, nontraditional responders will not be able to deduce the veiled meaning of phrases such as *management by objectives*, nor will they be able to recall the meaning of this concept when trying to keep track of the other thirteen management characteristics. Per NIMS doctrine, plain language is used to describe elements of the framework; however, the language often requires detailed and non-intuitive definitions.[4]

The term management by objectives, for example, seems straightforward. It seems to mean that a high value should be placed on establishing objectives that are used to set operational priorities, or even that response operations should be grouped into objectives and then coordinated by business stream. But these assumptions are false. Instead, the term has a complex and nuanced meaning that stakeholders must decode. Per the NIMS 2017 doctrine, management by objectives means:

- Establishing specific, measurable objectives;
- Identifying strategies, tactics, tasks, and activities to achieve the objectives;
- Developing and issuing assignments, plans, procedures, and protocols for various incident management functional elements to accomplish the identified tasks; and

[3] Leslie D. Lutz and Michael K. Lindell, "Incident Command System as a Response Model within Emergency Operations Centers during Hurricane Rita," *Journal of Contingencies and Crisis Management* 16, no. 3 (September 2008): 123, https://doi.org/10.1111/j.1468-5973.2008.00541.x.

[4] Federal Emergency Management Agency (FEMA), *National Incident Management System*, 3rd ed. (Washington, DC: Department of Homeland Security, 2017), 19, https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf.

- Documenting results against the objectives to measure performance, facilitate corrective actions, and inform development of incident objectives for the subsequent operational period.[5]

The first two bullets are a more refined definition, sourced from the common-sense interpretation of the term. The final two veer away from what could be considered common terminology and plain language, and into highly specific first responder vernacular. There are significant barriers for government departments, the private sector, and nongovernmental stakeholders to overcome if they wish to understand the elements of NIMS, let alone master them, to fully integrate into emergency response operations.

B. RESEARCH QUESTION

What is the ideal approach for local governments to take to include nontraditional stakeholders in incident response to a catastrophic disruption of critical infrastructure?

C. DEFINING THE PROBLEM SPACE: THE SOTHIRSTY SCENARIO

To help define the problem space, this thesis develops a scenario that presents a novel catastrophic event, and helps to explain why stakeholder engagement is important before and after a critical disruptive event. Developed by the author for the purpose of this thesis, the SoThirsty scenario is intended to add value for practitioners addressing challenges around incident response to a catastrophic critical infrastructure disruption.

While the nation has not yet experienced an incident like the one presented in the scenario, it draws from real-life circumstances. The 2018 cyber-attack against Atlanta, Georgia, and the 2018 and 2019 cyber-attacks against Baltimore, Maryland, show the scenario's plausibility.[6] These events show that a catastrophic attack against local governments—and, by association the 85 percent of critical water systems operated by

---

[5] FEMA, 21.

[6] Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," *New York Times*, March 27, 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html; Kimberly Eiten, "Baltimore Ransomware Attack: City Inches Closer to Normal Operations," CBS Baltimore, June 12, 2019, https://baltimore.cbslocal.com/2019/06/12/baltimore-ransomware-attack-inches-closer-to-normal/; "Baltimore's 911 Emergency System Hit by Cyberattack," NBCNews, March 28, 2018, https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876.

local governments—could trigger severe impacts.[7] Information drawn from the Incident Specific Preparedness Review for the Deepwater Horizon oil spill was used to show the value of developing a common operating picture.[8] Finally, the understanding that there is an essential need to incorporate the private sector into incident response operations has been growing within the emergency management field since the "2017 Hurricane Season FEMA After-Action Report" was issued. Since then, revisions of other guiding documents, like the draft version of the National Response Framework, have elevated the private sector's role. These documents, in addition to a variety of other open source materials and the author's unique understanding of potential impacts to the National Capital Region, were used to intricately weave together the elements of the scenario and identify likely impacts.

The SoThirsty scenario is complex by design, to highlight how various stakeholders may be engaged as such an incident unfolds. Furthermore, as with all scenario-driven exercises, some elements of reality are suspended to allow conversation to flow around the what-ifs and why-nots that the exercise aims to draw out. The series of sequential moves that unfold in vignettes, presented in Figure 1 and then in the figures at the start of each chapter (and compiled for ease of use in Appendix B), are set over the course of seven days. The timeframe is greatly expanded compared to common emergency management or cyber-based exercises; rarely do exercises tackle the challenges of response operations that are sustained over the course of a week or a month, as would be a reality during a cyber-attack against critical infrastructure.

---

[7] National Infrastructure Advisory Council, *Water Sector Resilience: Final Report and Recommendations* (Washington, DC: Department of Homeland Security, 2016), 3, https://www.dhs.gov/publication/niac-water-sector-resilience-final-report.

[8] Roger Rufe et al., *BP Deepwater Horizon Oil Spill Incident Specific Preparedness Review (ISPR): Final Report* (Washington, DC: U.S. Coast Guard, January 2011), 52.

SoThirsty Scenario Move 0 (00:01–00:30 Minutes)

On a warm day in June 2022, a disgruntled contractor working for the utility that provides drinking water to the National Capital Region (approx. 6 million people*) accesses an unattended water pumping station. The contractor releases the SoThirsty virus into the utility's industrial control systems, then departs for headquarters to turn in his letter of resignation.

Over the course of several weeks, the SoThirsty virus incrementally reduces the amount of chlorine released into the drinking water system. Chlorine treatment is the foundation of preventing waterborne diseases that cause illness or even death, like e. coli or cryptosporidium.** Since inspections on the water's conformity with standards are automated by industrial control systems, the changes in chlorine level go unnoticed by operators. The chemical formula used to prepare water to meet drinking standards is out of balance.

After four weeks, reports of strange-smelling drinking water trickle into the utility customer service line. Across the region, emergency departments are filling with patients with flu-like symptoms, some severe.*** Only when workers notice algae growing on water tanks are purity checks performed manually and the impacts of the contamination confirmed.

Upon this realization, the utility shuts down distribution until proper water treatment processes can be validated, to protect people from getting sick. Without water pressure, wastewater discharge services cease, causing sewage to back up in homes, office buildings, restaurants, hotels, and hospitals in the affected locations. Local hospitals experience a surge in patients with severe symptoms of e. coli and cryptosporidium illness. Due to a lack of water pressure, flights in and out of Reagan National Airport are suspended; without water pressure, fire suppression systems cannot be operated to meet federal aviation standards. During this time, the public expects service to be restored and potable water to flow from faucets.

At 06:00 hours after water distribution ceases, emergency declarations from impacted local governments start to be issued. Local governments open their emergency operations centers (EOCs) to manage the impacts of the water outage.

* Jeff Clabaugh, "Washington Metro Population Climbs to 6.2 Million," WTOP, March 22, 2018, https://wtop.com/business-finance/2018/03/washington-metro-population-climbs-to-6-2-million/.

** Chlorine Chemistry Council, "Drinking Water Chlorination: A Review of Disinfection Practices and Issues" (report, Chlorine Chemistry Council, 2003), 2, https://waterandhealth.org/wp-content/uploads/2017/04/dwwp.pdf.

*** Chlorine Chemistry Council.

Figure 1. SoThirsty Scenario Move 0 (00:01–00:30 Minutes)

Though the SoThirsty scenario asks the reader to suspend disbelief, the hypotheticals do not invalidate the points that are illustrated by the scenario's fact pattern and assumed outcomes. The scenario focuses readers on the real-world impacts of a major cyber-incident affecting industrial control systems that are operating critical infrastructure, and offers options to address the cascading effects; the "worst-case scenario" figures that accompany each scenario move show impacts that the infrastructure attack may have under current NIMS and ICS frameworks, while the "best-case scenario" figures show the more limited impacts of an improved framework designed to incorporate second- and third-tier responders. The scenarios and potential impacts are compiled in Appendix B. As the resources needed to respond to the real-world impacts of a catastrophic cyber-attack on critical infrastructure extend past those offered by first responders, the need to incorporate these new stakeholders into a management structure is essential. This thesis seeks to determine the attributes of a management framework that would allow for seamless integration of these new partners.

D. DEFINITIONS

The following terms are used throughout the thesis. The definitions are consistently used throughout Department of Homeland Security and other homeland security enterprise publications; the terminology in this thesis is intended to be compatible with existing definitions that are common to organizations with a homeland security mission.

- First responders: "those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers."[9]

- Second-tier responders/stakeholders: Representatives from governmental organizations whose responsibility to support incident response operations is only activated during an incident that exceeds first responders'

[9] White House, *National Preparedness*, Homeland Security Presidential Directive 8 (Washington, DC: White House, 2003), 18–22, https://www.hsdl.org/?view&did=441951.

capabilities.[10] These representatives' primary mission does not relate to supporting incident response operations, but they move into this role as their expertise is needed.

- Third-tier responders/stakeholders: Representatives from organizations with no responsibility to support incident response operations, generally conceptualized as the private sector or nongovernmental organizations. They generally have little to no exposure to incident response operations and are unfamiliar with existing protocols and procedures. An event with significant impacts (locally, regionally, or nationally) must occur for third-tier responders to be involved in incident response operations. The term is used in this thesis to denote groups that are in the private sector.[11]

- Jurisdiction: The lowest level of government in an impacted region—a city, county, or town, depending on the political makeup of the area.

E. METHODOLOGY

A narrative scenario approach is used in this thesis to evaluate NIMS's success in incorporating nontraditional stakeholders into response operations occurring at the local government level in emergency operations centers (EOCs). To create a frame of reference for a catastrophic attack against critical infrastructure that would necessitate the support of nontraditional stakeholders, this thesis employs the fictional SoThirsty scenario. Drawing elements from a variety of existing scenarios developed by state and federal government and private-sector subject matter experts, available through open sources, this research uses the scenario to test technical capabilities and frameworks that help to protect life safety. To better align with the research question, this thesis omits technical elements of the source scenarios.

---

[10] Definition adapted from Nicholas B. Hambridge, Arnold M. Howitt, and David W. Giles, "Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies," *Homeland Security Affairs* 13 (April 2017), https://www.hsaj.org/articles/13773.

[11] Definition adapted from Hambridge, Howitt, and Giles.

To determine the gaps in capability of the existing NIMS framework, this research also examines a breadth of academic articles and practitioner evaluations of NIMS. Significant writing addresses the qualities of NIMS, both generically and during implementation. This evaluation produces a collection of pathways and barriers to implementing NIMS for incidents that rely on traditional first responders (those from the fire service, law enforcement, and emergency medical services). Specifically, this evaluation examines NIMS's:

- Flexibility to integrate organizations without a life safety protection mission into response operations
- Capacity to integrate stakeholders who are unfamiliar with the NIMS structure
- Ability to support the unique needs of a catastrophic critical infrastructure outage

The information generated from these concepts is evaluated for patterns and commonalities. Understanding the flaws in NIMS implementation in traditional events will allow planners to discover its value during responses to nontraditional events. The thesis then applies the determined strengths and weaknesses of NIMS to the fictional scenario. This comparison illustrates the deficiencies in applying the NIMS framework to a catastrophic critical infrastructure outage.

Ultimately, this thesis aspires to make a valuable contribution to the literature of emergency response, to evaluate the applicability of NIMS for incidents that require nontraditional stakeholders, and to highlight the necessity of public-private partnerships before and during a catastrophic critical infrastructure outage. The intent is to directly inform the development of novel solutions to incident management for cyber-incidents impacting critical infrastructure outages. Though the impacts of such an attack are caused by the compromise of cyber-physical systems, this thesis is written for broad applicability to any catastrophic critical infrastructure outage. This thesis ultimately proposes a new conception of an incident response framework for local government EOCs that can be

employed during incident response to a catastrophic critical infrastructure failure, and offers a path forward for implementing the framework.

THIS PAGE INTENTIONALLY LEFT BLANK

II. UNTAPPED RESOURCES: THE INCIDENT RESPONSE SYSTEM AND NONTRADITIONAL STAKEHOLDERS

Figures 2 through 4 show the second scene in the SoThirsty scenario and its potential impacts, which unfold after the first thirty minutes and through the first day of the incident. See Appendix B for the compiled scenario moves.

SoThirsty Scenario Move 1 (00:30–24:00 Hours)

Immediately after the first reports of the water outage, sales of potable water surge in the impacted region. The news media issue reports of looting for potable water, though no evidence is produced. Establishments that still have water in stock request law enforcement support to quell disputes that store managers worry may grow into violence. Without water pressure, sanitation systems fail, leaving sewage backing up into homes and businesses. Those with the financial means travel outside the impacted region for medical treatment and to access drinking water and sanitation systems.

The water outage prevents hospitals and medical facilities from sanitizing instruments and surfaces, increasing the spread of bacteria. Hospitals throughout the region suspend operations and transfer patients out of the affected area, despite the surge in demand from patients suffering from exposure to e. coli and cryptosporidium. Due to the water outage, public health inspectors close restaurants; it is impossible to sanitize dishes and utensils, cooking tools, or perishables. Per regulation, fire marshals close schools and office buildings due to the lack of fire suppression and sanitation systems.

Reagan National Airport suspends operations once water pressure dwindles. Per regulation, without the mandated fire suppression capability, in-bound and out-bound flights must be halted. Immediately the air traffic infrastructure across the nation is plunged into disarray. Dozens of flights already in the air must be redirected to other airports. Future flights are delayed at first, only to be canceled. Thousands of passengers trying to get to Washington, DC, are stranded, and those whose planes or crew were coming from Washington, DC, are left grounded. By hour 24, the financial impacts incurred by airlines are significant, and they are rushing to upstaff their customer service support teams to mitigate damage to their brands due to customer outrage.

Validated information is slow to emerge from the water utility, and rumors are running wild both within the local government EOC and among the public. The public is calling 9-1-1 for more information about the incident, slowing response times to incidents threatening life safety. Major third-tier stakeholders and the federal government issue incorrect service restoration times based on news media reports, causing mass confusion and weakening the public's trust in the government.

Figure 2. SoThirsty Scenario Move 1 (00:30–24:00 Hours)

Worst-Case Scenario Impacts: Scenario Move 1

- Across the impacted region, EOCs use National Incident Management System (NIMS) and Incident Command System (ICS) processes to conduct operations. The operational battle rhythm and policies specific to EOCs are challenging for second- and third-tier responders to understand. Many have never been in an EOC and cannot determine what is expected of them or how to best support operations. Incident response operations slow considerably while emergency management staff members conduct just-in-time training. Second-tier responders are unfamiliar with the ICS forms and defer to their internal reporting systems, which are not standardized across stakeholders. The lack of standardization between the report formats takes significant effort to reconcile by EOC leadership.

- No mechanism exists to collect situational updates from the third-tier stakeholders, and limited personnel are assigned to this task.* There is no visibility on mid- and long-term issues that may arise, limiting the effectiveness of response operations. Without gathering situational awareness from third-tier stakeholders, EOC leaders are operating without a complete common operating picture. As a result, guidance issued by the responding jurisdictions is inaccurate or irrelevant, increasing the public's frustration.

- Third-tier representatives with resources to share do not know who to contact to participate in response operations, and grow frustrated.

- Requests are made to state-level emergency management organizations to procure potable water. These requests can be approved quickly, but there are delays in receiving the products. As local governments look to other solutions for rapid procurement, local government attorneys become significant players in expediting procurement of essential goods. Unfortunately, there are substantial legal barriers for collaboration that local governments and third-tier stakeholders must overcome. Without a way to expedite procurement of needed commodities, the willing and able vendors cannot assist with response operations through the government incident response framework.

* The Liaison Officer is the official NIMS/ICS position that supports engagement of nongovernmental stakeholders. FEMA, *National Incident Management System*, 3rd ed. (Washington, DC: Department of Homeland Security, 2017), https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf.

Figure 3. Worst-Case Impacts: SoThirsty Scenario Move 1

Best-Case Scenario Impacts: Scenario Move 1

- The policies and procedures used to operate EOCs reflect common sense, and novice responders are easy to incorporate. When second- and third-tier responders arrive at EOCs, they can quickly start contributing to developing a common operating picture. Throughout the EOC, visual prompts reinforce the common-sense structures used to organize operations.
- Local government attorneys have minimal challenges interfacing with the players at the EOC due to the easy-to-understand operational framework. The coordination of crisis procurement processes results in reduced bureaucratic red tape and expedites the procurement of critical resources.
- Some third-tier stakeholders are severely impacted by the incident; others are major players in response operations. Those with critical resources to share are eager to support incident response operations. When EOCs reach full operational status, virtual business emergency operations centers (BEOCs) are activated. The virtual format allows for a secure exchange between the EOC and third-tier stakeholders on issues specific to the private sector. Third-tier stakeholders quickly learn that the BEOC is the best avenue for accessing information about the incident and to facilitate resource sharing with other third-tier stakeholders and the EOC. Access to the BEOC is easily granted: interested parties can request access via the Office of Emergency Management's website.

Figure 4. Best-Case Impacts: SoThirsty Scenario Move 1

A. WICKED PROBLEMS

According to Svante Edzen, the conditions that create a wicked problem stem from highly complex deviations from normal operating conditions.[12] Wicked problems sit in contrast to tame problems, which have solutions that can be quickly identified, allowing for consensus to be reached by responders quickly.[13] Examples of tame problems include traffic accidents or kitchen fires; more complex challenges—like forest fires or airplane crashes, or a catastrophic water outage—present wicked challenges to responders due to

[12] Svante Edzen, "Table-Top Exercises for Emergency Management: Tame Solutions for Wicked Problems," *47th Hawaii International Conference on System Sciences* (2014): 1978, https://www.semanticscholar.org/paper/Table-Top-Exercises-for-Emergency-Management%3A-Tame-Edzen/2a4422445a3c25abec4744618aa115a5d9ca8c4c.

[13] Edzen, 1978.

their dynamics and complexity.[14] In these instances there is a great challenge to adopt a uniformly accepted understanding of the problem space and corresponding solutions to return operations to normal conditions.[15] Scenario Move 1 (Figure 2) presents an example of a wicked challenge: prioritizing and allocating resources. The impacts outlined are likely highly critical to each different stakeholder responsible for addressing the threat or hazard to their mission space.

Challenges to effective and efficient response operations can be attributed, at least in part, to Edzen's assertion that "the solution to a wicked problem uncovers new problems that require further adjustment of the solution."[16] Wicked problems require iterative processes and revision to address cascading impacts. As local government EOCs begin to conduct response operations, the impacts of the SoThirsty scenario spread like a web through the community. Once the impacts of the catastrophic water outage grow beyond the capabilities of traditional first responders, second- and third-tier stakeholders become the primary responding organizations: in the SoThirsty scenario, public health inspectors inform restaurants that they must close until water is restored to prevent foodborne illnesses, airlines must rebook passengers on a massive scale, medical facilities must direct patients to other service locations, and most significantly, the failure of sewage systems to transport and process human waste must be addressed by public health and public works departments who, in turn, rely on the private sector. EOCs in impacted jurisdictions must rush to develop a common operating picture of impacts and prioritize resource allocation. The worst-case impacts shown in Figure 3 illustrate the challenges that can arise without structural flexibility to incident response frameworks.

Efforts to stabilize the incident are conducted within the NIMS and ICS frameworks by organizations with the primary mission of ensuring life safety. The Department of Homeland Security and the Federal Emergency Management Agency (FEMA) instituted NIMS and ICS to prepare the nation to respond to "all incidents, regardless of size,

---

[14] Edzen, 1978.

[15] Edzen, 1978.

[16] Edzen, 1980.

complexity, or scope, and planned events."[17] The intended application of this definition is limited to events that are primarily dependent on traditional responders. In instances when groups other than law enforcement, the fire service, or emergency medical services are critically involved, existing incident response frameworks are structurally incapable of incorporating the necessary response resources. In the SoThirsty scenario, the mission space of first responders is quickly outpaced, and resources offered by second- and third-tier stakeholders are needed.

Challenges with the practical application of ICS and NIMS are also highlighted in academic discussion about the incorporation of second- and third-tier stakeholders into the response framework. Such academic conversation has focused primarily on incidents involving ICS that are supported by traditional, on-the-scene first responders, rather than incidents supported by an EOC. Dick Buck, Joseph Trainor, and Benigno Aguirre's discussion about the limitations of ICS, as expanded by Donald Moynihan, are the most substantial and comprehensive arguments that consider the framework's ability to integrate second- and third-tier stakeholders.[18] Ultimately, as an event becomes more dynamic via the inclusion of second- and third-tier stakeholders, NIMS and ICS are insufficient; however, there is not significant academic discussion on this topic.[19]

If the nation's leaders are to think strategically and manage wicked problems, they must have the opportunity to practice this type of processing; the existing emergency management doctrine, however, does not allow for such opportunities. An article for *Disaster Prevention and Management* explains that "the conventional disaster management cycle tends to be locked into a process of single-loop learning where the emphasis is on institutional resilience and improved performance within given parameters. This lacks the richness of local knowledge and experience necessary to build effective

---

[17] FEMA, *National Incident Management System*, 2.

[18] Dick Buck, Joseph Trainor, and Benigno Aguirre, "A Critical Evaluation of the Incident Command System and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006), https://doi.org/10.2202/1547-7355.1252; Donald Moynihan, "The Network Governance of Crisis Response: Case Studies of Incident Command Systems," *Journal of Public Administration Research and Theory* 19, no. 4 (October 2009): 897, https://www.jstor.org/stable/20627881.

[19] Lutz and Lindell, "Incident Command System as a Response Model," 124.

preparedness in responding to produced unknowns."[20] The authors argue that practice with responding to unknowns, rather than to expected results, will better prepare the whole community to respond to events.[21] This concept is valid within the perspective of exercise design and practices standard within emergency management.

B. WAR GAMING AS A TOOL FOR REAL PREPAREDNESS

The U.S. military has employed the strategy of war gaming, or thinking in an artificial context, to foster creative decision-making to address wicked problems on the battle field.[22] War gaming, as implemented by the Department of the Navy, references a variety of activities that span a range of participation types.[23] This range extends from discussion-based workshops that draw from subject matter experts' knowledge of a topic to two-sided gaming where each side of a conflict is staffed by a team of decision-makers who map out offensive or defensive moves.[24] With concepts that originate from strategic military thinking, the modern technical definition of war gaming is established in the Naval War College's *War Gamers' Handbook*.[25] The text describes war gaming as

> a tool for exploring decision-making possibilities in an environment with incomplete and imperfect information (Herman, Frost, & Kurtz, 2009). Additionally, a value unique to all war games is the occurrence of previously unknown issues, insights, or decisions that arise during the conduct of a game. War game participants may make decisions and take

---

[20] Geoff O'Brien et al., "Approaching Disaster Management through Social Learning," *Disaster Prevention and Management* 19, no. 4 (2010): 504, https://doi-org.libproxy.nps.edu/10.1108/09653561011070402.

[21] O'Brien et al., 505.

[22] Yuna Huh Wong et al., *Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action* (Santa Monica, CA: RAND, 2019), 17, https://www.rand.org/pubs/research_reports/RR2227.html.

[23] Shawn Burns, David Della Volpe, Robin Babb, Nick Miller, and Gordon Muir, *War Gamers' Handbook: A Guide for Professional War Gamers* (Newport, RI: U.S. Naval War College), 5, https://apps.dtic.mil/dtic/tr/fulltext/u2/1001766.pdf.

[24] Burns et al., 6; Yuna Huh Wong, "How Can Gaming Help test Your Theory?" *The RAND Blog*, May 18, 2016, https://www.rand.org/blog/2016/05/how-can-gaming-help-test-your-theory.html.

[25] Wong et al., *Next-Generation Wargaming*, 11; Burns et al., *War Gamers' Handbook*, 3.

> actions in a game that even they would not have anticipated, if not for the game environment (Perla, 1990).[26]

A significant value of war games is the opportunity to practice decision-making in the context of novel challenges. Simulations of offensive and defensive actions that help the players anticipate cascading impacts have helped military thinkers develop strategic plans for combat operations.

Historically, war gaming became a prominent strategic tool for military forces during World War 1.[27] The technique fell out of favor after the United States' failures in Vietnam, and as technological advances made it possible to integrate computer-based models into strategic planning.[28] In the twenty-first century,

> [a]s U.S. forces struggled in Afghanistan and Iraq, there was also increased concern that combat models, focused on physical performance of weapon systems, failed to capture the political and social dynamics that were actually driving events on the ground…. This effectively created two dueling cultures of gamers: those working on large statutory games or campaign modeling efforts tied to the programs of record and those working on smaller games to support specific studies and programs.[29]

The divergence that formed in war gaming methodology created two distinct objectives. The first aimed to test and evaluate previously developed plans and policies, also referred to as "programs of record."[30] The other objective focused on less formalized topics, preferring to draw data from academic studies and hypotheses rather than working around rigid parameters.

Within the emergency management field, war games, referred to as exercises, are at the core of preparedness. As the emergency management field incorporated the concept of war gaming, however, several core characteristics of the technique evolved away from its original intent. FEMA's approach to war gaming is dictated by Homeland Security

---

[26] Burns et al., *War Gamers' Handbook*, 5.

[27] Wong et al., *Next-Generation Wargaming*, 13.

[28] Wong et al., 15–17.

[29] Wong et al., 17.

[30] Wong et al., 17.

Exercise and Evaluation Program (HSEEP) doctrine. Implemented in 2013, HSEEP standardizes the policies and procedures used in the development, execution, and evaluation of exercises.[31] Instead of focusing on critical decision-making, HSEEP exercises aim "to test and validate [existing] plans and capabilities."[32] A critical difference between traditional war gaming and HSEEP exercises is the established objective.

Per the *War Gamers' Handbook*, on the other hand, war gaming focuses on addressing open-ended questions and fostering imaginative thinking to respond to novel challenges, including challenges that have never been faced in reality.[33] Simply, the value of war gaming comes from the opportunity for creativity. Rather than focusing on creativity, the HSEEP guidance states that exercises promote national preparedness "by enabling whole community stakeholders to test and validate plans and capabilities, and identify both capability gaps and areas for improvement."[34] This emphasis on validation of plans and capabilities is fundamentally different from the emphasis in traditional war gaming; an emphasis on affirming rote decision-making removes the opportunity for the players to critically prepare for truly novel events that present wicked problems.

The SoThirsty scenario illustrates the variety of challenges that responders might face in the event of a catastrophic water outage. During this low-probability but high-impact event, wicked problems develop in every direction; there is no clear, singular way to define the challenge at hand. Due to the scale of the event at almost every turn, several wicked problems grow out of previously made decisions. In this light, the scenario serves two purposes: first, it is a scenario template that emergency managers can adapt for their own application (see Appendix A) in order to spur conversation around wicked problems; second, as the scenario develops in the scenes presented at the beginning of each chapter in this thesis (and as compiled in Appendix B), the reader is presented with an illustration

---

[31] FEMA, "Homeland Security Exercise and Evaluation Program, 2013" (report, Department of Homeland Security, 2013), 1, https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

[32] FEMA, 1.

[33] Burns et al., *War Gamers' Handbook*, 3.

[34] FEMA, "Homeland Security Exercise and Evaluation Program," 1.

of potential cascading impacts from wicked problems, showing the vulnerabilities in existing incident response frameworks. The challenges emphasized in the scenario are systemic and thus would arise in any large-scale disruptive incident.

The root of these vulnerabilities and challenges can be traced back to ICS, which is the framework for both planning and responding to incidents. As wicked problems surface during a crisis, "the enormous variety of circumstances" mean that "no single framework of steps is likely to prove useful in all situations."[35] Rather than open-ended simulations that reward creativity, rely on unscripted methodology, and promote decision-making, emergency management war gaming has become an exercise in plan validation and routine execution, in large part due to the application of ICS .

C. THE APPLICATION OF ICS TO CATASTROPHIC INCIDENTS

An emerging body of literature advocates against the utility of ICS for complex incidents. In their 2006 article, "A Critical Evaluation of the Incident Command System and NIMS," Buck, Trainor, and Aguirre argue that ICS in its traditional conception is only a useful framework during precise, situationally dependent events. The authors posit that less dynamic incidents, those only requiring participation by a few stakeholders, can use ICS effectively to manage incident operations.[36] Specifically, they stress that ICS can be successful during events that are "repetitive, limited in their operative goals, scope, duration, and are often events for which community organizations have trained together and devised a predetermined division of labor and a set of formal and informal procedures that facilitate their successful implementation."[37] Gregory Bigley and Karlene Roberts state that ICS is highly flexible, but their consideration of its flexibility extends only to organizations that have emergency-management or incident-response-related teams, such

---

[35] Charles I. Stubbart, "Uncertainty, Complexity, Conflicts of Interest, Emotional Involvement, and the Quality of Crisis Thinking" (faculty working paper, University of Illinois at Urbana-Champaign, September 1986), 33, https://www.ideals.illinois.edu/bitstream/handle/2142/27634/uncertaintycompl1289stub.pdf?sequence=1&isAllowed=y.

[36] Buck, Trainor, and Aguirre, "Critical Evaluation."

[37] Buck, Trainor, and Aguirre, 14.

as the Federal Aviation Administration or the Red Cross, further reinforcing the point that the system is valuable only for those groups familiar with its concepts and practices.[38]

Buck, Trainor, and Aguirre further note that as an incident becomes more complex, and as resources are needed from groups not traditionally included in incident response, the utility of ICS declines.[39] When capabilities and stakeholders are limited during response operations, ICS's command-and-control management model works well; when the scope is broader, however, and the volume of essential responders increases, the rigidity of ICS limits its effectiveness as a response framework.[40] The "tight discipline" and rigid infrastructure that characterize traditional first responders' policies and procedures make ICS a compatible structure with preexisting operational frameworks.[41] But as rigidity works to strengthen first responders' connection with ICS, it alienates "normal civilian structures, such as public works and social services, [which] cannot operate as effectively under such a structure."[42] This inability to integrate other stakeholders is a limitation of ICS—and by extension, NIMS—that reduces the efficacy of these models for critical infrastructure incidents.

As illustrated in the SoThirsty scenario, a wide range of resources are needed from a diverse group of second- and third-tier responders to support response operations to a catastrophic water outage. In this instance, only a small operational footprint for traditional first responders exists. If the scenario were to occur today, the organizations defined as second- and third-tier stakeholders would be forced to mold themselves into the inflexible ICS framework, leading to failure or significant delays in resource delivery. Buck, Trainor, and Aguirre state that "for ICS to be effective as a tool to coordinate the response, it must be used by a community of official responders who through training and shared

---

[38] Gregory Bigley and Karlene Roberts, "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments," *Academy of Management Journal* 44, no. 6 (2017): 1283–84, https://doi.org/10.5465/3069401.

[39] Buck, Trainor, and Aguirre, "Critical Evaluation," 14.

[40] Buck, Trainor, and Aguirre, 14.

[41] Lutz and Lindell, "Incident Command System as a Response Model," 123.

[42] Lutz and Lindell, 123.

experiences, over years of public service develop technical confidence and interpersonal trust in each other."[43] To facilitate developing these relationships, the authors assert that nontraditional stakeholders from government organizations and the private sector may be involved in response operations in large-scale emergencies, though they must be exposed to the principles and practices of ICS to normalize their role within the framework.[44] Without the flexibility to include a diverse and educated range of incident responders, ICS is not an effective framework for incident response to a catastrophic attack against critical infrastructure. As incidents increasingly involve nontraditional stakeholders, the utility of ICS and NIMS declines.

D. ICS AS A NETWORK RATHER THAN A HIERARCHY

When incident response involves stakeholders other than first responders, the response framework needs different characteristics than those prescribed in ICS to be successful. In a 2008 article, Moynihan accepted Buck, Trainor, and Aguirre's findings and evaluated the ways the ICS structure can be adapted during implementation. In Moynihan's view, practitioners (first responders) agree that ICS is a hierarchical system and that the command-and-control framework is necessary for the successful management of an incident.[45] Kathleen Tierney and Joseph Trainor disagree, however, stating that incident response operations must be decentralized—a need that was present during the response operations at the World Trade Center on 9/11.[46] Moynihan's conclusion is that the centralization of authority, a hallmark of NIMS and ICS, will break down effective

---

[43] Buck, Trainor, and Aguirre, "Critical Evaluation," 14; Lutz and Lindell, "Incident Command System as a Response Model," 124.

[44] Buck, Trainor, and Aguirre, "Critical Evaluation," 21; Lutz and Lindell, "Incident Command System as a Response Model," 123–24.

[45] Moynihan, "Network Governance of Crisis Response," 897.

[46] Kathleen Tierney and Joseph Trainor, "Networks and Resilience in the World Trade Center Disaster," in *MCEER: Research Progress and Accomplishments 2003–2004* (Buffalo, NY: University of Buffalo, 2004), 163, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.537.5317&rep=rep1&type=pdf.

decision-making processes when there is no clear hierarchy, as is the case with incidents that span a large geographical area or that rely heavily on nontraditional stakeholders.[47]

As illustrated in the SoThirsty scenario, there is a great need for collaboration and integration of resources from nontraditional stakeholders during a crisis. At the same time, a crisis requires someone to take command and, in some instances, sometime to be responsible for decision-making.[48] To evaluate the different schools of thought, Moynihan considers the role of urgency in decision-making during a crisis:

> The centralization imperative for crisis response is urgency. When combined with the need for a network of interdependent responders, urgency creates a coordination problem. Gradual processes of interorganizational consensus building and mutual adjustment take too long. Responders need a central coordinating mechanism to direct resources and resolve conflict in a timely fashion.[49]

If the urgency of a crisis forces a hierarchical approach for decision-making, it seems antithetical that urgency would also necessitate centralized decision-making. This exemplifies the argument between practitioners and academics around the topic of effective decision-making.[50] Ultimately, Moynihan—opposing Tierney and Trainor's conceptual framework—concludes that a network governance approach can dually meet the needs of centralization and urgency if ICS is reconceptualized "as a highly centralized mode of network governance, designed to coordinate interdependent responders under urgent conditions."[51] The discussion that follows accepts the new conception of ICS as a form of network governance rather than a hierarchy and explores the new definition.

A network governance approach challenges these competing perspectives (command and control of an incident versus the incorporation of second- and third-tier

---

[47] Moynihan, "Network Governance of Crisis Response," 897.

[48] William L. Waugh Jr. and Gregory Streib, "Collaboration and Leadership for Effective Emergency Management," *Public Administration Review* 66, no. s1 (December 2006): 138, https://doi.org/10.1111/j.1540-6210.2006.00673.x.

[49] Moynihan, "Network Governance of Crisis Response," 898.

[50] Moynihan, 898.

[51] Moynihan, 898; Tierney and Trainor, "Networks and Resilience," 164.

stakeholders) by recasting ICS as a formal mechanism to foster network coordination. This approach recognizes that a network can be governed via centralized mechanisms while also acknowledging the complexities created by the network setting.[52] Moynihan reviews case studies to explore how a crisis affects ICS as a network.[53] His first finding validates Buck, Trainor, and Aguirre's central argument that it is difficult to incorporate emergent responders into ICS.[54] His second finding reveals that networks, by definition, do not have a primary leader; instead, control is shared between several stakeholders.[55] He further notes that as the size and scope of a crisis expands to include nontraditional stakeholders, operations become more networked and decentralized.[56]

E. PRACTICAL CHALLENGES TO THE IMPLEMENTATION OF NIMS AND ICS

In a research project for the National Fire Academy, Dana Cole evaluated ICS from its beginnings in the 1970s to 2000, just a few years before its national implementation through NIMS.[57] Prior to its national implementation, ICS had been battle-tested by the fire service in California for decades and, starting in 1982, was incorporated into the National Fire Academy's curriculum.[58] As Cole discusses, there are several systemic challenges to overcome through the implementation process, some of which were identified before the system's national adoption.

A significant hurdle to the successful implementation of ICS at the individual and organizational level is the challenge around terminology and the standardization of concepts. Cole details that these challenges "necessitate a virtual translation of

---

[52] Michael McGuire, "Collaborative Public Management: Assessing What We Know and How We Know It," *Public Administration Review* 66, no. s1 (December 2006): 42, 33–43, https://doi.org/10.1111/j.1540-6210.2006.00664.x.

[53] Moynihan, "Network Governance of Crisis Response," 901–2.

[54] Moynihan, 903.

[55] Moynihan, 906.

[56] Moynihan, 906.

[57] Dana Cole, "The Incident Command System: A 25-Year Evaluation by California Practitioners" (research project, National Fire Academy, 2000), 203, https://www.hsdl.org/?view&did=454470.

[58] Cole, 209.

terminology, principles, and working relationship to those cooperators who have little to no experience with ICS."[59] ICS terminology and concepts—and particularly their nuances—are challenging to understand without a background in the fire service. Without an easy-to-understand structure and continual exposure to the concepts, committing ICS to memory is incredibly challenging, which significantly limits the system's effectiveness.

It is also challenging to retain information without real-life applications for that information. Cole states that "one of the primary reasons that the ICS model works so well is that it is continually 'practiced and performed.'"[60] Second- and their-tier stakeholders who do not use ICS regularly, however, will need additional assistance to work successfully within the framework. A respondent in Lutz and Lindell's study about the value of ICS as a model for response operations in EOCs during Hurricane Rita expanded on this sentiment:

> I am not familiar with ICS in a practical sense. I have been involved in training but they [sic] are very dry. I would be interested in a mentoring program where individuals not familiar could use the "buddy" system to walk thru [sic] a "typical" event with others who have the real life application.[61]

Cole places a particular emphasis, as well, on "growing pains" for law enforcement entities and nongovernmental agencies that are working to adopt ICS.[62] In 2000, Cole attributed these challenges to the translation adopters must perform to understand the fire-service-based framework and content.[63] To motivate individuals or organizations to overcome the fire-service-based structure and adopt ICS when it was first rolled out, Cole says it needed to be apparent that this new incident management framework would provide significant value and safety.[64]

---

[59] Cole, 210, citing Senge.

[60] Cole, 223.

[61] Lutz and Lindell, "Incident Command System," 132.

[62] Cole, "Incident Command System"; Lutz and Lindell, "Incident Command System," 132.

[63] Cole, "Incident Command System," 210.

[64] Cole, 210.

A detailed review of the literature produced no significant sources that address the challenges posed in the research question—In what ways can local governments better incorporate nontraditional stakeholders during incident response operations that do not rely primarily on traditional first responders? While there is extensive writing on the utility of NIMS and ICS at an incident scene, as implemented by first responders, the academic discussion is scarce around the application of NIMS and ICS for incidents being managed from an EOC by second- and third-tier responders.[65] The lack of significant sources further motivates the research question and the work presented in this thesis, as well as additional investigations into this area.

F. CONCLUSION

There are significant conceptual gaps in the incorporation of second- and third-tier stakeholders into ICS. In the event that nontraditional stakeholders are able to achieve proficiency in the framework, there are additional hurdles to incorporation. This illustrates that ICS is structurally closed off to incorporating second- and third-tier stakeholders.

As the effects of the SoThirsty virus hypothetically spread through the impacted communities, the need for first responders diminishes, and second- and third-tier responders are increasingly needed. These responders, however, are to set up for failure if they are organized through NIMS and ICS. Cole's discussion of the range of complications to successful implementation of ICS clarifies the practical challenges responders face—primarily, that, unless it is used on a regular basis, ICS needs to be translated into layman's terms.[66] For second- and third-tier stakeholders, this presents a significant challenge. By definition, these groups do not participate in incident response operations on a regular basis, which makes ICS an unrealistic approach for them.

While the texts featured in this chapter have established the limitations of NIMS and ICS, their analysis does not cover all the limitations the frameworks would encounter if applied to a prolonged incident like the one in the SoThirsty scenario. The following

---

[65] Bigley and Roberts, "Incident Command System," 1281.

[66] Cole, "Incident Command System."

chapter builds off of this work by examining the flaws of the current management framework and identifying subphases that exist within incident response. The severity of the impact from the water outage in SoThirsty will only grow as the incident does, and developing a framework to incorporate all critical stakeholders is essential, but currently structurally impossible, for ICS and NIMS.

III. OUT WITH THE OLD, IN WITH THE NEW: TRANSITIONING AWAY FROM ICS

Figures 5 through 7 show the third scene in the SoThirsty scenario and its potential impacts, which unfold after the first seventy-two hours of the incident. See Appendix B for the compiled scenario moves.

SoThirsty Scenario Move 2 (72:00 Hours)

The water outage continues. Without drinking water, functioning sanitation systems, or medical services, those with the ability to do so are fleeing the region. The mass migration has triggered a run on gasoline. Stations are rushing to restock fuel but the demand exceeds the supply chain's capacity.

The news media has released more reports of looting, and smartphone video footage shows people breaking into grocery stores looking for bottled water. Reports state that some stores in the impacted region are selling a case of bottled water for over $75. The most vulnerable members of society, those without the resources to leave the impacted region, are still without access to drinking water. Emergency management officials are still securing potable water resources for those who cannot travel to access water.

Heating, ventilation, and air conditioning systems cannot operate without water, and plumbing systems stop working. As a result, office buildings close, displacing almost 1.3 million employees supporting the federal government mission from their worksites.* Some organizations direct staff to telework. Network servers in impacted office buildings must be powered down to avoid overheating, limiting the ability to conduct day-to-day operations via telework. Small businesses that rely on foot traffic around office buildings worry about their businesses' viability during a prolonged period of decreased customers.

Hotels in the impacted area are vacant, including 33,000 rooms in Washington, DC.** Hotels and restaurants are closed and have laid off all shift workers until water is restored. As a result of school closures due to the water outage, students who rely on low- and no-cost lunch and breakfast programs go without meals.

* Jeff Clabaugh, "Exactly How Many Washingtonians Work for the Federal Government?" WTOP, February 19, 2018, https://wtop.com/business-finance/2018/02/exactly-many-washingtonians-work-federal-government/.

** "Washington, DC Visitation and Impact (2017)," Destination DC, accessed February 25, 2020, https://washington-org.s3.amazonaws.com/s3fs-public/2017_visitor_fact_sheet.pdf.

Figure 5. SoThirsty Scenario Move 2 (72:00 Hours)

Worst-Case Scenario Impacts: Scenario Move 2

- Third-tier stakeholders want to leverage their resources but have not been able to find the appropriate contact within the EOC. Instead, these actors create their own water distribution systems. Swarms of people quickly overwhelm distributors, creating a fertile ground for riots to develop. Urgent 9-1-1 calls requesting law enforcement support spike and divert resources from other critical law enforcement activities.
- Without a mechanism to gather information from third-tier stakeholders, to include nonprofit organizations, incident responders cannot anticipate the need to provide supplemental meals to students who rely on school meal programs until the situation has already grown into a crisis.
- Though there is a great need to facilitate refueling of gas stations, there is no infrastructure in place to begin a conversation with the necessary stakeholders for status updates and other situational awareness. Many station owners would gladly report the volume of customers they are seeing and keep EOC leadership up to date with shipment delivery times, but they are unaware there is a need for this information.
- Overly optimistic restoration times issued by the government frustrate third-tier stakeholders who would have otherwise acted to mitigate the impacts of the water outage on their business. As a result, representatives from corporations in the impacted area reach out to politicians to ask for more comprehensive updates. Meeting each of these requests detracts from EOC leadership's ability to focus on response operations, further delaying the development of a comprehensive common operating picture.
- Second-tier stakeholders in the EOC are frustrated by NIMS regulations. The operational tempo and ICS forms seem to be in a foreign language.

Figure 6. Worst-Case Impacts: SoThirsty Scenario Move 2

Best-Case Scenario Impacts: Scenario Move 2

- As it becomes apparent that an unofficial evacuation is occurring, EOC leadership reaches out to the business community via the BEOC to identify any known leaders within the convenience and fuel retailing community. Within hours the EOC has a few contacts who can provide status updates from their networks, greatly contributing to a common operating picture. Information is easily exchanged via the BEOC.
- Third-tier stakeholders with extensive supply chain networks access bulk drinking water supplies and connect with response personnel via the BEOC.
- Second- and third-tier community-based stakeholders have checked in with the populations they serve and their synthesized information has been incorporated into the common operating picture. Several issues are identified as they are forming, allowing responders to take action and mitigate the impacts before they escalate. As a result of these community-based organizations' incorporation into incident response operations, the EOC coordinates with social services and third-tier stakeholders to organize free breakfast and lunch services for students who qualify, as schools are not in session.
- As new nontraditional responders cycle into the EOC, the easy-to-understand procedures prevent a need for just-in-time training.

Figure 7. Best-Case Impacts: SoThirsty Scenario Move 2

As the SoThirsty water outage wears on, people become more desperate for help, and faith in the government's capacity to manage the incident starts to dwindle. Although some second-tier organizations have NIMS and ICS training, they are not familiar enough with the concepts or policies to integrate into the organizational framework easily. Instead of coordinating resources effectively, their focus is being pulled away from the mission at hand to ensure they comply with official NIMS regulations. In part, they try to decipher the ICS incident forms, a tool designed for use at incident scenes during field operations owned by first responders, making the integration into EOC operations challenging. Third-tier stakeholders, the private sector and nongovernmental organizations, are trying to access official response operations to share their resources. NIMS and ICS do not sufficiently provide the needed organizational features to support the cascading impacts of the SoThirsty attack on critical infrastructure.

NIMS was intended to be an incident management system for all types of incidents, but it was never intended to incorporate nontraditional stakeholders as primary responders. Arguably, the framework's architects had a specific type of incident in mind when it was designed: incidents like 9/11 that primarily rely on first responders. Nontraditional stakeholders with critical resources need to play a more active and formal role in incident response to support communities during response operations. The larger an event, the greater the resources needed, and the more critical the second- and third-tier stakeholders' role in incident response. Under this premise, this chapter explores the subphases that comprise incident response operations. This discussion illuminates the space within response operations where second- and third-tier stakeholders can be incorporated.

A. NIMS AND ICS: IMPERFECT SYSTEMS

NIMS intends to ease the friction around sharing resources, managing an incident with responses from different departments or jurisdictions, and ensuring synchronized communications to inform decision-makers and the public. This desire developed following 9/11, when the federal government's goal was to increase interoperability between jurisdictions to better neutralize threats and hazards.[67] Homeland Security Presidential Directive 5, issued in February of 2003, declared NIMS aimed to be the national incident management framework that would facilitate resource sharing from the federal government to states and localities when the resource demands exceed their local capability.[68] Initially released in 2004 by the Department of Homeland Security, NIMS is the framework that federal, state, local, tribal, and territorial governments must follow to facilitate interoperability of resources, communications, and personnel management during incident response.[69] NIMS is not an operational or tactical guide to address emergency incidents; it is a management framework to organize resources and communications and

[67] Andrew C. Teeter, "On A Clear Day, You Can See ICS: The Dying Art of Incident Command and the Normal Accident of NIMS—A Policy Analysis" (master's thesis, Naval Postgraduate School, 2013), 18–19, https://www.hsdl.org/?view&did=736338.

[68] White House, *National Preparedness*, 1.

[69] FEMA, *National Incident Management System*, 1.

manage incident response.[70] The management framework characterized by ICS is the primary conceptual framework that built NIMS.

As previously discussed, the now standardized ICS emerged from best practices developed by the fire service in California during the 1970s and became adopted voluntarily across the nation in the following decades.[71] Prior to adoption of ICS, efforts to contain and extinguish massive wildfires in California struggled:

> Sometimes, fire units from different jurisdictions passed each other without communicating—even though one was heading to put out a fire in the sector the unit they passed has just come from. Some sectors were overlooked because everyone thought others were taking care of those sectors. On the whole, no fire department knew what the others had done, were doing, or planned to do.[72]

Following California's severe 1970 fire season, seven fire organizations from across the state worked together under the Firefighting Resources of Southern California Organized for Potential Emergencies (FIRESCOPE) program to develop strategies to mitigate the impacts of severe wildfires by strengthening coordination of response operations through standardization.[73] The FIRESCOPE program standardized incident management structures and established common terminology, processes, and a management framework.[74] The concepts established in ICS were exported to national firefighting organizations as early as 1982 at the National Fire Academy.[75] Not until the *9/11 Commission Report*, released in 2004, and the establishment of NIMS that same year, was

---

[70] FEMA, 1.

[71] Cole, "Incident Command System," 207.

[72] Lutz and Lindell, "Incident Command System," 123.

[73] Cole, "Incident Command System," 207; Lutz and Lindell, "Incident Command System," 122.

[74] FEMA, *National Incident Management System*, 3–4; Lutz and Lindell, "Incident Command System," 123.

[75] Teeter, "On A Clear Day, You Can See ICS," 16; Cole, "Incident Command System," 209.

ICS nationally standardized, mandated, and implemented as a framework for all hazards, rather than just fire-based emergencies.[76]

In his master's thesis, Andrew Teeter suggests that the national mood in the years following the 9/11 attacks was sensitive to righting the perceived failures of the response efforts, and ICS was the answer.[77] The *9/11 Commission Report*'s recommendation on the matter states: "Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response."[78] After this endorsement of ICS, and in addition to the direction issued through Homeland Security Presidential Directive 5 in 2003, the national adoption of ICS and NIMS was put into motion.[79] The 9/11 Commission members considered emergency measures in keeping with the themes of 9/11, understandably. Their concerns arose from preventing another similar tragedy, which was novel at the time, and the framework they suggested therefore fit the needs of response to a mass casualty incident, for which response operations are primarily handled by law enforcement and the fire service.

Today, the United States still faces these threats and hazards, but first responders have trained and prepared for them. Although the national incident response framework has been refined over the years since its implementation, its utility still applies to events with first responders as the primary responding entities. Lutz and Lindell reiterate this in their conclusion, stating that "ICS was originally designed to structure onscene operations in structural and wildland fires, not EOC operations in other types of incidents."[80] The primary responders needed to support the impacts of the SoThirsty scenario cannot be successfully incorporated into the existing management structure. If local governments are

---

[76] National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report*, 397; "National Incident Management System (NIMS) Fact Sheet," Department of Homeland Security, accessed February 28, 2020, https://www.fema.gov/pdf/emergency/nims/NIMSFactSheet.pdf.

[77] Teeter, "On a Clear Day, You Can See ICS," 18–19.

[78] National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report*, 397.

[79] White House, *National Preparedness*, 1.

[80] Lutz and Lindell, "Incident Command System," 132.

prohibited from using inclusive approaches to coordinate incident response operations, to include developing their own EOC procedures, then the nation will be vulnerable to the potentially catastrophic impacts of a critical infrastructure outage.

B. EXPANDING THE UNDERSTANDING OF THE RESPONSE PHASE

As the nation faces novel, long-term incidents such as a catastrophic critical infrastructure outage, we must expand the conceptual timescale of incident response from forty-eight or seventy-two hours to a much longer time frame of weeks to months. Often, conventional wisdom suggests that this longer timeline should transition operations into the recovery phase, but this is incorrect. The National Preparedness Goal defines the incident response mission area as performing activities that "save lives, protect property and the environment, and meet basic human needs after an incident has occurred."[81] For natural, human-made, and technological incidents, the activities that achieve this are defined as: "saving and sustaining lives, stabilizing the incident, rapidly meeting basic human needs, restoring basic services and technologies, restoring community functionality, providing universal accessibility, establishing a safe and secure environment, and supporting the transition to recovery."[82] Understanding of the parameters of the response phase allows us to see that incident response does not need to be limited to traditional first responders, and helps us understand the critical role an EOC plays.

The strategic value of an EOC during incident response operations, for both those with and without an incident scene, cannot be understated. Michael Ryan, writing for *Technological Forecasting and Social Change*, states that in an EOC, "the immediate goal is to anticipate the needs of the future, so that they can be addressed immediately in order to save lies and protect property."[83] There are five primary functions that occur in an EOC that are necessary to achieve this: collaboration, policy making, operations management,

---

[81] Department of Homeland Security, *National Preparedness Goal*, 2nd ed. (Washington, DC: Department of Homeland Security, 2015), 12, https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf.

[82] Department of Homeland Security, 12.

[83] Michael Ryan, "Planning in the Emergency Operations Center," *Technological Forecasting and Social Change* 80, no. 9 (November 2013): 1729, https://doi.org/10.1016/j.techfore.2013.01.006.

information gathering, and support for elected officials.[84] These functions can only be performed successfully when they originate from a collaborative mindset—not from a mindset of command and control, the guiding ethos for NIMS and ICS.[85]

Examining the response phase more closely and identifying its subphases can help to determine access points for second- and third-tier stakeholders, and can also help showcase the role of an EOC. It can offer, as well, insight into the value of ICS for response activities that are not conducted by traditional first responders. Harrald consider the response phase as being divided into the four subsections shown in Figure 8, which are characterized by a diversity of activities.

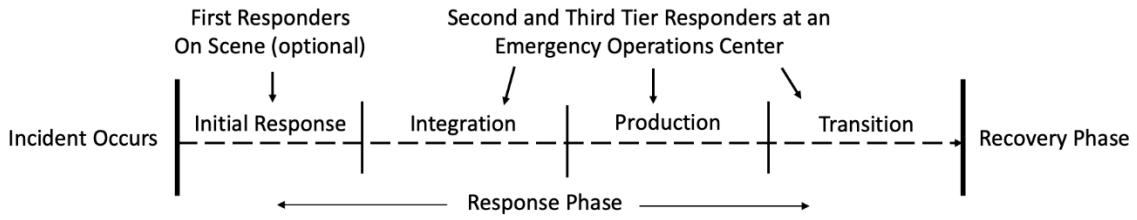

Figure 8. Response Phase Subsections[86]

Immediately after an incident occurs, operations are characterized by the initial response phase. The initial response phase is immediate and short-term, and NIMS should be used to organize operations that support stabilizing life safety. These are the activities performed by traditional first responders to neutralize the threat or hazard, such as running into a burning building or neutralizing an active shooter.[87] For the majority of events, this is the

---

[84] Ronald Perry, "The Structure and Function of Community Emergency Operations Centres," *Disaster Prevention and Management* 4, no. 5 (1995): 39–41, https://www.researchgate.net/publication/297655226_The_structure_and_function_of_community_emergency_operations_centres.

[85] E.L. Quarantelli, "Ten Criteria For Evaluating The Management of Community Disasters," *Disasters* 21, no. 1 (March 1997): 48, https://doi-org.libproxy.nps.edu/10.1111/1467-7717.00043.

[86] Adapted from John R. Harrald, "Agility and Discipline: Critical Success Factors for Disaster Response," *The Annals of the American Academy of Political and Social Science* 604 (March 2006): 260, https://www-jstor-org.libproxy.nps.edu/stable/25097791.

[87] Harrald, 260.

only phase of response operations that occurs. For a minority of events, however, additional resources required to respond to the threat or hazard are mobilizing as the second phase of Harrald's construct is activated.[88]

The integration phase provides a structure for the organization of external resources.[89] At this point in response operations, there is a path for incorporation of second- and third-tier stakeholders. Harrald sees this phase as "required to structure these resources into a functioning organization capable of identifying needs and providing services that are beyond the capability and capacity of the early responders."[90] This requirement aligns with the operational space that defines EOCs; an EOC is a central hub for information sharing, and for facilitating resource coordination during incident response operations.[91]

Without engaged representatives from response organization, an EOC is nothing more than a computer lab; with proper representation, however, as allowed by Harrald's structure, the integration phase turns an EOC into "the master coordination … point for all counterdisaster efforts."[92] The integration phase highlights the opportunity to include second- and third-tier stakeholders. During this phase, as highlighted in Scenario Moves 2 and 3 (Figures 5 and 9; see also Appendix B), EOCs are taking stock of the situation, and determining what resources are needed and from where they can be sourced. Ideally, second- and third-tier stakeholders would be incorporated at this time. Currently, however, NIMS does not allow for this. Traditionally the same management structure that is used by the NIMS Command and Coordination section to manage incident command is employed at an EOC. The primary benefit, FEMA argues, is that mirroring the incident command

---

[88] Harrald, 260.

[89] Harrald, 260.

[90] Harrald, 260.

[91] FEMA, *National Incident Management System*, 35.

[92] Quarantelli, "Ten Criteria," 51–52; Perry, "Community Emergency Operations Centres"; Thomas E. Drabek and Gerald J. Hoetmer (eds.), "Managing Disaster Response Operations," in *Emergency Management: Principles and Practice for Local Government* (Washington, DC: International City Management Association, 1991), 201–23.

structure reduced friction between the responders.[93] For incidents that do not require first responders, incident command operations should automatically flow into an EOC that is organized to facilitate incorporation of second- and third-tier stakeholders.

Harrald makes two points to support his discussion that the integration phase necessitates support from the second- and third-tier stakeholders. First, he argues that operations are being performed with participation from multiple organizations when a "coordinated multiorganization, networked response system is established."[94] This discussion implies that responsibilities for response efforts include entities other than traditional first responders—as opposed to during the initial response phase, which must be owned by the organizations performing the activities, most commonly traditional first responders. At this point, the need for ICS diminishes. The characteristics of NIMS and ICS only subtract from the efficiency of coordinating resources. Thus, when operations move into the integration phase, they should be transitioned to an EOC. And second, Harrald advocates for a networked approach, rather than a hierarchical one, to the integration phase.[95] This concept has already been validated by Moynihan's discussion of ICS's weakness when it comes to incorporation of nontraditional first responders.[96]

The need to incorporate nontraditional responders into EOC operations continues to grow once initial incident impacts are identified and the response operations transition into the production phase. Now two steps away from the initial response phase, the production phase occurs when "the response organization is fully productive, delivering needed services as a matter of routine."[97] This is well illustrated in Scenario Move 3 (see Figure 9, at the beginning of the next chapter), when critical response activities have been identified, including those only uncovered through cascading impacts, and solutions are in place. For example, by this time in the SoThirsty scenario, water distribution protocols

---

[93] FEMA, *National Incident Management System*, 35.

[94] Harrald, "Agility and Discipline," 262.

[95] Harrald, 262.

[96] Moynihan, "Network Governance of Crisis Response."

[97] Harrald, 262.

have been put in place and adjusted to meet the needs of the incident. Finally, operations move into the transition phase, which is preparation for the recovery phase.[98]

Harrald's deconstruction of the response phase of incident operations—which is unique among the literature—establishes the breadth of activities that occur during a response effort. By defining the initial response, integration, production, and transition phases, he creates the space to evaluate how operations can best be orchestrated. Without question, NIMS and ICS have a place in the initial response phase; the urgent requirement to neutralize threats and hazards is almost ubiquitous with first responders' mission. This utility of these frameworks is limited, though, when operations move into the integration and production phases. As illustrated in the SoThirsty scenario, when considering the impacts of a catastrophic incident with a long-term response phase, there is a great need to involve second- and third-tier stakeholders. Activities like procuring potable water and providing food pantry support to workers who have been laid off from service industry jobs cannot be coordinated by first responders. This is not a part of their mission space and, as compared to the second- and third-tier organizations that specialize in providing these types of services, they lack the necessary expertise.

C. CONCLUSION

As the nation faces novel vulnerabilities and the role of first responders in incident response operations declines, there is an opportunity to reconceptualize incident response operations. Under Harrald's structure, the primacy of first responders' role can subside, depending on the incident characteristics, after life safety is stabilized during the initial response phase. In the context of the SoThirsty scenario there is a great need for coordination following the stabilization of life safety, and a diverse group of stakeholders, both those impacted and those with resources to contribute, need to be incorporated.

During the best-case scenario impacts for each SoThirsty scenario move (Figures 3, 6, and 10; see also Appendix B), EOC leadership has made the decision to include a wide range of second- and third-tier stakeholders in EOC operations. The decision to

[98] Harrald, "Agility and Discipline," 262.

incorporate school systems and nonprofits facilitates the identification of a critical cascading impact of the water outage. Students who rely on low- or no-cost breakfast and lunch are going without food due to the school closure. Ultimately, the worst-case scenario impacts (Figures 4, 7, and 11; see also Appendix B), which arise from the NIMS and ICS structures, are not inclusive in incident response membership; stakeholders in these cases realize the impacts, but only once these impacts create their own crises, which trigger a much larger and more urgent allocation of resources. This example illustrates the value of information gathering to inform priorities for response operations.

IV. COMPONENTS FOR A NEW APPROACH

Figures 9 through 11 show the final scene in the SoThirsty scenario and its potential impacts, which unfold after the seventh day of the incident. See Appendix B for the compiled scenario moves.

SoThirsty Scenario Move 3 (Day 7)

Water service has not been restored at this time. Office buildings, hotels, and restaurants remain closed. Much of the population in the impacted area has evacuated the region. The exodus has reduced the demand for goods significantly, and grocery and convenience stores close indefinitely. As a result, regular donations to food banks are suspended, making the impacts of the water outage disproportionately severe for those who rely on social support services. Many members of the same population rely on shift work from hospitality industry jobs from which they have been laid off due to business closures. By day seven, vulnerable populations have been thrust from a difficult situation into a dire one.

The repercussions of the water outage have permeated the nation. The store closures have halted the flow of goods into the region and caused delays across the country. Major corporations are reimagining their supply lines to avoid the impacted region and work to develop strategies to store the unsold goods. Freight that would normally travel by truck through the Mid-Atlantic region is diverted, impacting business along the major transportation corridors.

Air traffic operations have been restructured to omit Reagan National Airport from routes. The planes and crews that comprised the almost 400 departures per day have been reallocated to other routes.*

The federal government has fully activated its continuity of operations plans and transitioned the majority of government functions to other parts of the country.

* "Washington, DC Visitation and Impact (2017)," Destination DC, accessed February 25, 2020, https://washington-org.s3.amazonaws.com/s3fs-public/2017_visitor_fact_sheet.pdf.

Figure 9. SoThirsty Scenario Move 3 (Day 7)

Worst-Case Scenario Impacts: Scenario Move 3

- Though there is a keen interest by third-tier stakeholders to contribute to response operations, the rigidity of NIMS goes against the business community's get-it-done ethos. When third-tier stakeholders are invited into the EOC or included in conference calls, the NIMS format is so foreign and technical that it is difficult to understand, and the formality seems unnecessary considering the urgency of the conditions.
- Pressure on politicians is mounting. Third-tier stakeholders are concerned about the government's capacity to effectively manage the incident and they are not hesitant to voice their frustrations. It is perceived that government operations have not considered the value the third-tier stakeholders bring to support incident response operations. EOC leadership diverts significant attention to respond to requests for information from politicians.
- EOC leadership is relying on man-on-the-street news reports from local business owners for specific updates on the business community's impacts.
- The need to provide breakfast and lunch to students who rely on school-based programs has grown to a crisis. Efforts at the EOC have shifted the focus from supporting the incident at large to prioritizing this issue.

Figure 10. Worst-Case Impacts: SoThirsty Scenario Move 3

Best-Case Scenario Impacts: Scenario Move 3

- With up-to-date and comprehensive information gathered from the BEOC about the extent of the impacts on third-tier stakeholders, EOC leadership assembles a more complete common operating picture.
- Second- and third-tier stakeholders see that, unless service industry employees can go back to work quickly, the cascading financial impacts may exceed the damage the water outage itself causes. Not only will the viability of businesses be threatened but employees who are at risk of missing a paycheck will need supplemental assistance. Recommendations are made to EOC leadership about the best courses of action to mitigate the cascading impacts.
- Local food banks are put on notice and are bracing for significantly higher-than-average customer demand and a decrease in available resources due to grocery store closures. With the advance warning, the organizations have time to use their connections to try to procure the needed resources.

Figure 11. Best-Case Impacts: SoThirsty Scenario Move 3

The SoThirsty scenario's worst-case impacts (for example, those shown in Figure 10) illustrate the challenges that arise from the application of NIMS and ICS to an incident that does not primarily rely on first responders. Inaccurate or out-of-date information is collected and disseminated, and opportunities to address impacts before they grow into crisis are invisible to EOC staff, all a result of the structural barriers inherent in NIMS and ICS that bar successful integration of second- and third-tier stakeholders. As the scenario moves unfold, EOCs are strained to identify and procure needed resources. The last-minute efforts to organize supplemental breakfast and lunch assistance to students is the most poignant example. For local governments to successfully manage incident response operations that do not primarily rely on first responders, an alternative to NIMS and ICS, as illustrated in the best-case scenario impacts, must be implemented.

The best-case track of the scenario (shown, for example, in Figure 11) illustrates a more inclusive approach to second- and third-tier stakeholders. Early on during incident response operations, EOCs on the best-case track in the SoThirsty scenario take advantage of the BEOC structure to cast a wide net, to include a variety of third-tier stakeholders. Easy-to-understand EOC policies used during incident response operations on this track facilitate the incorporation of second- and third-tier stakeholders. These processes, alternatives to NIMS and ICS, provide a comprehensive and accurate snapshot of the effects of the water outage.

Discarding NIMS and ICS expands the opportunity to identify elements for a successful incident command system for local government EOCs. Rather than a dictated framework like NIMS and ICS, a customizable structure must be established to serve as a guide for local governments. The pillars of a new framework become evident in both the worst- and best-case response tracks. The SoThirsty scenario highlights five elements, or capabilities, to guide local government emergency managers to optimize incident response operations for a catastrophic attack against critical infrastructure: an established common operating picture, incorporation of the right stakeholders, the ability to do business with the private sector, easy-to-understand information-sharing practices, and regional coordination and communication.

A. FIVE CAPABILITIES

The five attributes highlighted in the SoThirsty scenario delineate the distinction between positive and negative management of an event that primarily relies on second- and third-tier responders. These capabilities are validated by the author's professional experience working as an emergency manager in the National Capital Region and by academic training. From these experiences, and in conjunction with the research performed for this thesis, the concepts described in this section were developed. They describe the essential factors for success during the response operations of an attack on critical infrastructure. Some of the capabilities may be familiar to those in the emergency management field and others may be novel; ideally, they all make common sense.

1. An Established, Comprehensive Common Operating Picture through Information Sharing

It is crucial to develop a common operating picture (COP) during response operations; only from this point can all other actions can progress. A COP sets the tone for urgency and, by establishing a shared understanding of incident characteristics, helps responders prioritize resource allocations during incident response operations.[99] Developing a COP involves collecting and synthesizing information to create a greater understanding of the incident's impacts. As illustrated in the SoThirsty scenario, impacts to the community are not immediately apparent, as they would be in an airplane crash or structure fire. Instead, EOC staff must seek out information from partners; it is therefore essential to establish an EOC-based infrastructure for information gathering and sharing.[100] Consistently, the SoThirsty scenario illustrates the limitation of NIMS and ICS to incorporate the stakeholders to create a full picture of impacts.

The NIMS-based version of the scenario impacts—shown in the worst-case impact figures throughout the thesis and in Appendix B—misses critical pieces of information

---

[99] Laura G. Militello et al., "Information Flow during Crisis Management: Challenges to Coordination in the Emergency Operations Center," *Cognition, Technology and Work* 9 (2007): 28, https://doi.org/10.1007/s10111-006-0059-3.

[100] Ryan, "Planning in the Emergency Operations Center," 1729.

early on, limiting the validity of the COP. As the scenario moves unfolded in the worst-case tracks, responders consistently work without current or comprehensive data, resulting in a delayed or inadequate response. The primary example of this is seen in Move 2, at seventy-two hours (see Figures 5 through 7 in Chapter III; also shown in Appendix B), when the inclusion of nontraditional stakeholders expedites the identification of a critical issue around school closures. Students who rely on free lunch and breakfast go longer without food assistance in the worst-case track. Furthermore, the delay in identifying the issue heightens the urgency of the situation, which triggers a higher-intensity response. The reallocation of efforts detracts from other facets of incident response, leaving areas with the potential for tangible negative impacts unattended. The best-case track's structural features, however, allow for incorporation of second- and third-tier stakeholders, who provide the needed visibility to gather a wide range of inputs to develop a comprehensive COP.

The wide-net approach to gathering information does have pitfalls. A legitimate concern about the efficacy of this approach is that the volume of data collected is so extensive that it is impossible to process it all under time constraints. Furthermore, it could be argued that the amount of information would dilute emphasis on the community's most critical needs, or even obscure the reality of the COP. Grouping stakeholders by area of responsibility or functional area can significantly mitigate these challenges and, if handled correctly, can resolve issues of "stovepipeing."[101] Creating a structure that allows for each area of response operations to represent its larger functional group can streamline and sculpt efficient and useful contributions to the COP. The FEMA Community Lifelines approach could be useful; this approach segments recovery efforts into seven critical service groups.[102] Each jurisdiction, on a case-by-case basis, must determine the best model to organize the collection and synthesis of information to create a COP, and then disseminate the information to relevant stakeholders. The success of the wide-net approach,

---

[101] Militello et al., "Information Flow during Crisis Management," 31.

[102] See "Community Lifelines," FEMA, accessed February 29, 2020, https://www.fema.gov/media-library-data/1544469177002-251a503b3717f0d6d483bae6169f4106/Revised_Community_Lifelines_Information_Sheet.pdf.

however, is dependent on having the right people at the EOC to represent each organization, both to contribute to the COP and to put the analysis drawn from the COP into practice to support response operations.

2. The Right People at the Table

The term *the right people* refers to stakeholders that embody a range of characteristics that will make them successful in their role as a responder. Generically this includes the ability to stay calm in high-pressure conditions and strong interpersonal skills that facilitate collaboration. Two additional elements stand out as essential for successful participation in emergency response operations. First, representatives in the EOC must have an accurate understanding of their organization's capabilities.[103] And second, in what might seem to be a contrary requirement, the representatives must also have authorization to make decisions about the allocation of resources. Both components are essential to deploying the needed resources in a timely fashion to meet urgent needs during incident response.

Representatives in the EOC must make informed, capability-based decisions and must therefore also possess a deep technical understanding of their functional area.[104] The subtext of this capability is that senior executives are not likely the right fit to support EOC operations. EOCs need to be staffed by representatives from second- and third-tier response organizations who understand the complexities of the challenges at hand and the full extent of their organizations' capabilities and limitations. Without an understanding of the boost-on-the-ground reality, executives may over-commit their resources or not be able to contribute to the technical discussion of the issues at hand. Furthermore, there is little time to run decisions up the chain of command during incident response operations. Representatives in the EOC must therefore be empowered in their position as a representative of their organization.[105] Without authority, operational progress can slow to a crawl and hinder the activities of other stakeholders, who may be reliant on the delayed

---

[103] Quarantelli, "Ten Criteria," 52.

[104] Quarantelli, 52.

[105] Quarantelli, 52.

organization. As EOCs work with second- and third-tier stakeholders, they must stress the importance of representatives with in-depth technical knowledge and with the authorization to make resource allocations and tactical choices.

The process of identifying the right people is challenging; in some instances, it may be necessary to accommodate representatives that do not meet the established criteria. Developing relationships with second- and third-tier stakeholders before an incident can be an antidote to some of the challenges that arise around not having the right people at the EOC. In part, establishing expectations for responsibilities, operational flow, and collaborative decision-making can prepare nontraditional responders for an a high stress experience and net positive results. Socializing incident response concepts and EOC policies and procedures before an incident can also facilitate discussion of resource sharing from the private sector to local governments. Efforts to bring the right people to the table should include outreach for procurement and finance staff from local governments.

3. Government's Ability to Do Business with the Private Sector

Outside of emergency conditions, the lines of responsibility between the private and public sectors are regulated by statutory authority, procurement policies, and contractual relationships. E.L. Quarantelli states that friction can arise when "the outsider relief group [a third-tier stakeholder] is attempting the same tasks as a local group [a second-tier stakeholder], there are likely to be questions about its legitimacy, authority, and decision-making."[106] To combat the potential for conflict around the overlapping mission space, stakeholders must work together before an incident occurs to resolve questions about roles and responsibilities during incident response operations. A first step to achieve this is to remove barriers for collaboration between the private and public sectors.

The SoThirsty scenario highlights the immediate demand for relaxed procurement policies at the local government level; bottled water is needed faster than state-level emergency management organizations can deliver it. During emergency incidents, standard procurement practices slow down the acquisition of essential supplies and services

[106] Quarantelli, 47.

and directly hinder the whole-community response process. Relaxed procurement regulations during an emergency will accelerate the delivery of much-needed supplies and services to those impacted by a catastrophic incident. The source of these types of delays is multifaceted, but is based in the technical policies and procedures governments employ to protect against fraud, waste, abuse, legal liability, and similar concerns. Traditional procurement policies and protocols assure that the goods and services being purchased are what they are advertised to be, and that they are of quality. Under normal operating conditions these considerations are critical to ensure governments are good stewards of public resources. Under emergency conditions, however, adjustments must be made to prioritize procurement of supplies and personnel needed to support emergency response operations. Prior to a crisis, jurisdictions must explore, on a case-by-case basis, how they will need to adjust their practices to determine an acceptable level of risk, and put an official policy in place.

4. Easy-to-Understand Information-Sharing Practices

NIMS characterizes itself as an easy-to-understand framework that relies on "common terminology and plain language" to facilitate communications and information sharing between responders from a range of backgrounds.[107] To optimize incident response operations, however, communications between relevant stakeholders must be developed to focus on the substance of the information shared rather than the methods used to share the information.[108] The "common terminology" prescribed by NIMS is a comprehensive, colloquial language that has been developed and refined with each revised version of NIMS issued by FEMA.[109] However, that language is rife with acronyms and terms that have highly specific and intentional definitions, which presents a significant challenge for second- and third-tier stakeholders as they work to integrate into an EOC. If the intent is to develop a framework to incorporate stakeholders who do not traditionally interface with the incident response apparatus, then adjustments must be made to lower the

---

[107] FEMA, *National Incident Management System*, 20, 57.

[108] Quarantelli, "Ten Criteria," 45.

[109] FEMA, *National Incident Management System*, 20.

barrier to entry by removing misleading terminology. Adjustments of this nature are needed to facilitate sufficient information sharing, a critical part of successful incident response operations.[110] While the terminology in NIMS is, itself, problematic, so too is the operational rhythm and the way it is communicated to second- and third-tier stakeholders.

In its present form, the Planning "P," a construct used in the 2017 version of NIMS, is an additional barrier to incorporating second- and third-tier responders into EOC operations. The Planning P, shown in Figure 12, establishes the operational pattern used in an EOC and details the required actions the EOC must take, in sequence.[111] Each advancement along the P's timeline is labeled with a vague term that must be decoded through additional research into the NIMS doctrine. This construct focuses more on directing how and when information should be shared rather than what the relevant information is.[112]

---

[110] Quarantelli, "Ten Criteria," 45.

[111] FEMA, *National Incident Management System*, 106.

[112] Quarantelli, "Ten Criteria," 45.

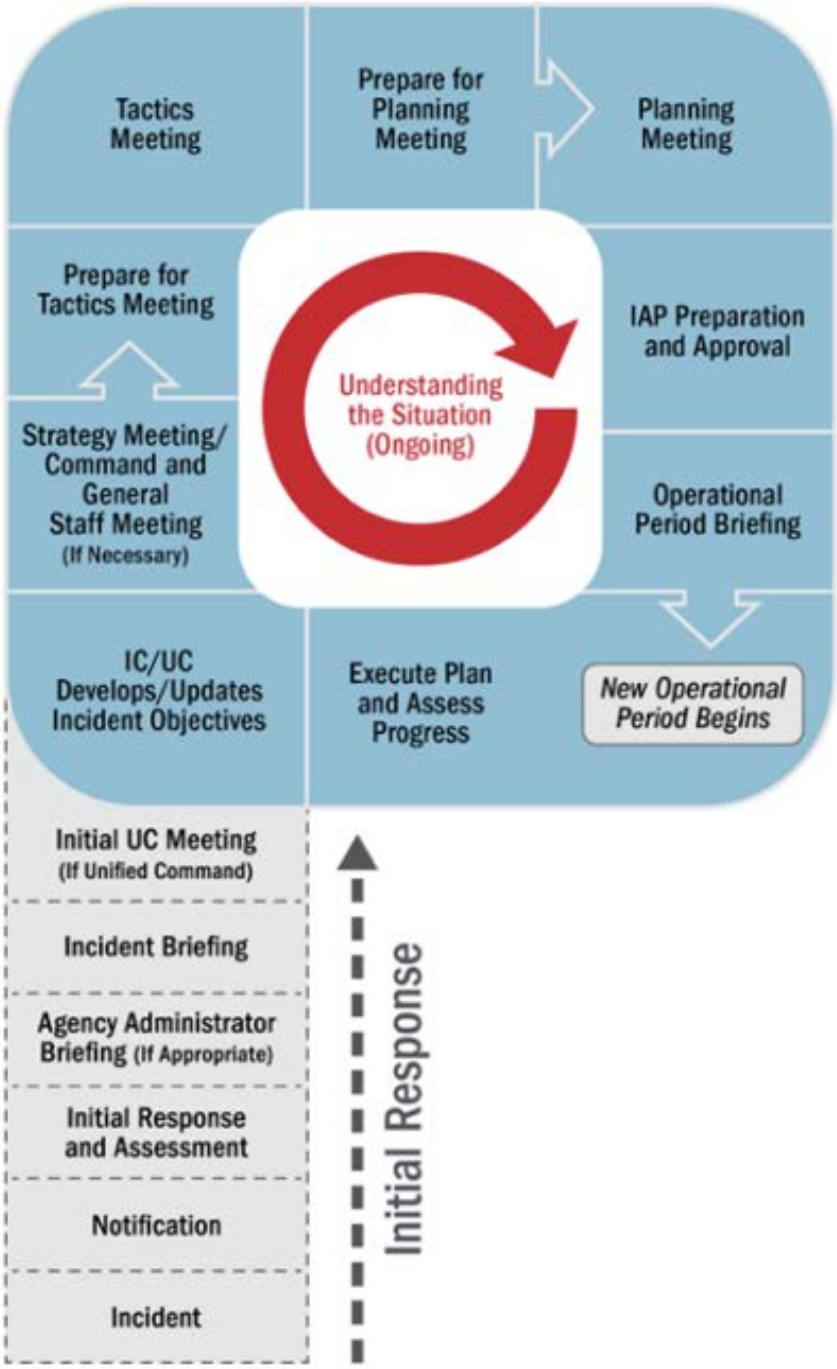

Figure 12. NIMS Planning "P"[113]

[113] Source: FEMA, *National Incident Management System*, 106.

There are alternatives to the Planning P, however, that achieve the same outcomes and that are far more accessible for second- and third-tier stakeholders; an example can be seen in Figure 13. This revised version of the Planning P uses common-sense terminology to communicate the organizational structure and responsibilities of each representative in an EOC. The revised Planning P also adjusts the objectives of each subphase of incident response to remove the holdover terminology and concepts from first-responder-based field operational battle rhythms. Due to its plain language, the revised Planning P places emphasis on the content of the information being shared rather than the technicalities of how it should be shared. This common-sense and approachable framework, or one similar, should be incorporated into operating guidelines for local EOCs to ensure the successful integration of nontraditional responders.

Assuredly, allowing jurisdictions to develop an EOC management framework that suits their organization's unique needs could create challenges to interoperability. Currently, All-Hazard Incident Management Teams or other support teams dispatched to relieve local EOC staff expect each EOC to comply with the standard NIMS structure to facilitate a smooth integration. Inevitably, if an EOC can use common-sense policies to incorporate second- and third-tier stakeholders logically, the same result would occur for supplemental EOC support teams. To link together operations from a variety of impacted jurisdictions, EOCs need to connect with their neighbors via a unified framework that minimizes the potential for miscommunication between local government EOCs.

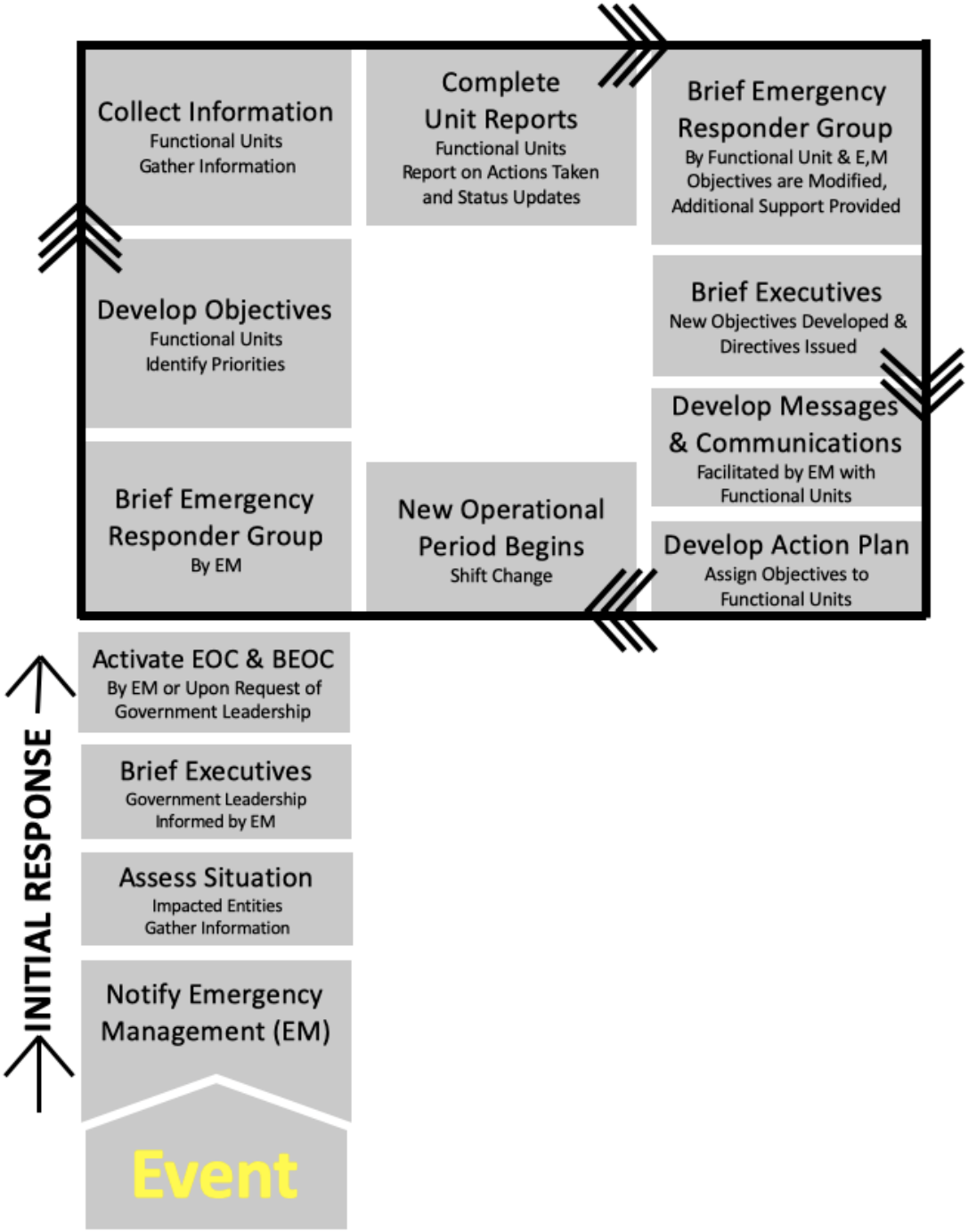

Figure 13. Amended Planning "P"[114]

[114] Source: Zachary Pope, email to author, May 17, 2019.

5. Regional Coordination and Communication

Despite the recommendation that EOC operations shift away from NIMS, the overarching ethos should remain intact: coordination between different responding groups must be facilitated. During a widespread incident, coordination and communication between impacted local government EOCs' response efforts will grind to a halt without coordination. Under these conditions, resource sharing will be severely hindered. To combat this, EOCs must consider the ways they will communicate with their neighbors and any overarching regional coordinating groups during active and steady-state operations. A collaborative approach between involved jurisdictions is essential to achieve the needed regional coordination to ensure successful information sharing and resource sharing.

Many regions across the nation have adopted policies for regional coordination, including, King County, Washington's, Regional Coordination Framework; the Kansas City Metropolitan Area Regional Coordination Guide; and the National Capital Region's Regional Emergency Coordination Plan.[115] Each of these documents serves a similar purpose: to implement communication protocols, delegate authorities, and establish decision-making bodies should the impacts of an event exceed the capability of a single or few responding jurisdictions. The capacity for regional coordination is essential to address the threats and hazards facing the nation today. The SoThirsty scenario is a great example of the interconnected nature of critical infrastructure and the potential catastrophic impacts in the event of an outage that extends beyond the boundaries of a single municipality or jurisdiction.

---

[115] "Regional Coordination Framework," King County, last updated July 25, 2019, https://www.kingcounty.gov/depts/emergency-management/emergency-management-professionals/regional-coordination-framework.aspx; "Regional Coordination Guide," MARC, accessed May 22, 2020, https://www.marc.org/Emergency-Services-9-1-1/MEMC/Other-Resources/Regional-Coordination-Guide; "Regional Emergency Coordination Plan," Metropolitan Washingotn Council of Governments, September 30, 2011, https://www.mwcog.org/file.aspx?A=l0xxarxHU0rCeawz0pCqkmn0rOQ1yOwK9ZoyvJUFCh4%3D.

B. CONCLUSION

The five capabilities highlighted in this chapter emphasize essential considerations for local government EOCs that are developing new policies and procedures. Rather than hard-and-fast rules, they are intended to serve as a guide, or a starting point for discussion. Ultimately, the conclusions drawn by each jurisdiction will need to be the result of collaborative work to identify the characteristics that best define the EOC's structure to reflect the their government structure, staffing levels, and other such considerations. At the local government level, EOCs need to create policies and procedures that facilitate incorporation of stakeholders other than first responders. Several recommendations in the following chapter serve as a road map for implementation of an alternate incident response framework for local government EOCs during response operations to a catastrophic critical infrastructure outage.

V. CONCLUSION: DIRECTION FOR STRUCTURAL CHANGE

This thesis sought to answer an important research question: What is the ideal approach for local governments to take to include nontraditional stakeholders in incident response to a catastrophic disruption of critical infrastructure? In answering this question, the thesis aimed to probe a previously unexplored problem space—that is, when incident response operations extend past stabilizing life safety and the response timeframe extends from hours to days, and even weeks, how are second- and third-tier stakeholders incorporated into response operations? Or more precisely, when the resources brought to the table by second- and third-tier stakeholders become more relevant than those offered by first responders, how is the management structure shifted to accommodate them? The research question posed by this thesis does not question the legitimacy of NIMS and ICS for first responders, but it does seek to create a more fitting framework for an emerging emergency situation.

To provide greater definition to this problem space, the thesis developed the SoThirsty scenario, presented piece by piece throughout the chapters as the scenario progressed by hours or days, and as the impacts grew more severe. Following a mass exodus of residents due to the water outage in the scenario, the most vulnerable members of the community were left behind. Grocery stores and hospitals closed, cutting those with the fewest resources off from critical lifelines. The business community sustained considerable impacts as well. The water outage forced the shutdown of heating, ventilation, and air conditioning systems, and disabled fire-suppression systems, making offices inhabitable for the few workers who chose not to evacuate the region. The best- and worst-case scenario impacts that accompany each scenario move provide rich detail into the drawbacks of NIMS as a response framework for this type of novel incident, and the benefits of adopting an alternative approach. At each turn during the SoThirsty scenario, the use of NIMS and ICS in EOC operations was outpaced by an alternative and decidedly more inclusive approach.

A. FINDINGS

Despite their national implementation and usefulness elsewhere, NIMS and ICS are not suitable for incident response operations that rely on nontraditional responders. The SoThirsty scenario depicts shows that, for this type of response, the need for second- and third-tier responders grows immensely as the emergency wears on. It becomes clear that NIMS and ICS fail to support local governments working to respond to a catastrophic critical infrastructure outage. These frameworks are limited because they were created for the threats and hazards that were most pressing when they were developed—events that primarily rely on traditional first responders. The *9/11 Commission Report*'s recommendation to implement ICS nationally validates this aim.[116] NIMS and ICS were intended to suit the needs of first responders during field operations, where there are criteria and conditions distinct from those of a catastrophic critical infrastructure outage, as illustrated in the SoThirsty scenario.

The origin of ICS in California's fire service is a further source of the structural inflexibility that limits the incorporation of second- and third-tier stakeholders. The original intention, per the FIRESCOPE project, was to standardize management of complex incidents at an incident scene.[117] This necessitates a hierarchical approach. In an incident like the one in the SoThirsty scenario, as the authority of first responders diminishes, there is an increasing need for flexibility and coordination between distinct groups and for an incident response structure that suits the parameters of an EOC. Groups that do not regularly operate in the incident response mission space cannot be expected to integrate into the hierarchy of ICS.

Aligning Harrald's model of incident response with the SoThirsty scenario creates the opportunity to incorporate nontraditional stakeholders into incident response operations. Harrald's depiction of the response phase as four subphases repositions stabilization of life safety as one element of response operations, rather than their

---

[116] National Commission on Terrorist Attacks upon the United States, *9/11 Commission Report*, 397.

[117] FEMA, *National Incident Management System*, 3–4; Lutz and Lindell, "Incident Command System," 123.

totality.[118] Defining integration, production, and transition as phases where response operations are performed, but not necessarily those based on protecting life safety in the immediacy, creates the opportunity to shift ownership of response operations away from first responders and to those who have subject matter expertise for the types of activities being performed.

B. CONCLUSIONS

For local government EOCs to best manage a response to a critical infrastructure outage, they must diverge from NIMS and ICS. And better alternatives do exist. Rather than mandating the implementation of another one-size-fits-all incident response doctrine, however, a more individualized approach should take shape. Upon departure from the standardized NIMS and ICS policies and procedures, jurisdictions will need to explore alternative incident response structures based on the five capabilities discussed in this thesis. The flexibility to incorporate these capabilities into incident response operations in a way that complements existing jurisdictional operations is a critical key to successful incident management.

The SoThirsty scenario and the corresponding best- and worst-case impacts illuminated five structural features that contribute to successful incident response to such events. These capabilities can guide emergency managers who are working to develop policies and procedures that suit them, their whole community, and their stakeholders. The five capabilities are:

- *An established, comprehensive common operating picture through information sharing*: Jurisdictions must develop infrastructure capable of gathering information to feed into a common operating picture from a wide range of sources.

[118] Harrald, "Agility and Discipline," 260.

- *The right people at the table*: Representatives in the EOC must have a tactical understanding of their organization's capabilities and the authorization to make decisions about resource allocation.

- *Government's ability to do business with the private sector*: Government entities must establish protocols prior to an emergency incident that facilitate resource sharing and procurement of goods from the private sector.

- *Easy-to-understand information-sharing practices*: Common-sense terminology and concepts must be used to convey the organizational structure and responsibilities of each representative in an EOC.

- *Regional coordination and communication*: Inter-jurisdictional communication and coordination is a critical element of incident response operations, regardless of jurisdictional EOC structures.

These capabilities should serve as a guide for local governments to identify defining policies and procedures of EOC operations. The authority to design EOC functions and policies should reside with local governments. Local governments should be able to operate their EOCs in the way that works best for them and all their stakeholders, and allows for adaptability based on incident characteristics.

Effective management of an incident like the one in the SoThirsty scenario requires collaboration and flexibility. Rather than mandating compliance with NIMS and ICS—frameworks intended for first responders and that have highly technical characteristics—a common-sense model that is developed by each jurisdiction's emergency management personnel should be developed for EOCs, and it should include policies that are easy to understand and incorporate. The resources that can be brought to bear by second- and third-tier stakeholders can have an enormous impact on response efforts and should not be omitted due to administrative road blocks. To leverage these resources, the incident management mentality needs to shift from a hierarchical structure to a partnership-based model—a shift that must start at the core of the emergency management field.

C. RECOMMENDATIONS FOR STRUCTURAL CHANGE

The following recommendations are intended to provide direction for EOCs that are developing incident management frameworks for critical infrastructure emergencies, and to answer the research question posed in this thesis.

1. Establish Emergency Management as a Field Independent of First Responders

Emergency management personnel are not first responders. Until this difference is recognized enterprise-wide, the incorporation of nontraditional stakeholders in incident response will stall, leaving precious critical resources unutilized during a crisis. Many of the challenges with NIMS and ICS's application to the SoThirsty scenario can be attributed to the original intent of the incident management systems—they are systems created by first responders, for first responders, to address incident scenes that are focused on protecting and stabilizing life safety. Using an incident response framework that can only be understood by one group of stakeholders reflects a lack of imagination around the types of threats and hazards the nation is facing today. There are many incidents that require emergency management personnel to partner with traditional first responders; when first responders are the primary stakeholders, it makes sense to continue to use NIMS and ICS.

Using NIMS and ICS exclusively for all types of incidents, however, is a siloed approach to preparing for emergency incidents that goes against the foundational concepts of emergency management. FEMA, along with a wide selection of professional emergency management associations, developed a document that provides an overview of the field's principles and values. This document includes the field's official mission statement, which defines emergency management as a field that "protects communities by coordinating and integrating all activities necessary to build, sustain, and improve the capability to mitigate against, prepare for, response to, and recovery from threatened or actual natural disasters, acts of terrorisms, or other man-made disasters."[119] The document goes on to outline eight

[119] "Emergency Management: Definition, Vision, Mission, Principles," FEMA, accessed February 29, 2020, https://training.fema.gov/hiedu/docs/emprinciples/0907_176%20em%20principles12x18v2f%20johnson%20(w-o%20draft).pdf.

principles, four of which are directly related to collaboration. This definition of the emergency management mission space necessitates collaboration with a range of partners before, during, and after an incident, and includes large representation from government organizations, the private sector, and community groups. Looking outside of response operations at the full spectrum of an incident—including mitigation, preparedness, response, and recovery—the overlap with traditional first responders pales in comparison to that with second- and third-tier responders.

2. Authorize Local Governments to Develop EOC Policies and Procedures Specific to Their Needs

Jurisdictions of different sizes, from megacities with hundreds of trained emergency management staff members to rural jurisdictions with only a part-time emergency manager, have different needs from an incident response management system. Some jurisdictions need to outline roles and responsibilities in order to group and delegate responsibilities among a large staff, while others need help defining the roles and responsibilities they can reasonably fill during an emergency. Adaptations to the implementation of NIMS and ICS in EOCs are likely happening unofficially already. Every local government EOC that does not have the personnel to fully staff ICS, or abandons the Planning P, shows an instance in which the formal structures are being reworked to suit resource constraints and better judgement. While replacing NIMS and ICS with another inflexible structure is counterproductive, there is a great need to provide guidance on how EOCs should be operated.

A departure from NIMS and ICS does not remove the necessity of sharing best practices to conduct EOC operations at the local government level. Rural, urban, and suburban emergency management departments will need guidelines and case studies to help determine best practices for their respective EOCs. FEMA is the natural body to provide this guidance. The organization's nationwide presence and strong administrative capacity to develop doctrine and similar types of operational guidance makes it the best fit. The national infrastructure can be leveraged to develop concepts built off of the five capabilities included in this thesis. With the staffing and resources available to FEMA, a comprehensive nationwide evaluation of best practices, development of case studies, and

the opportunity for community feedback can be achieved. This guidance will be a critical starting point for local governments that wish to plan EOC policies and procedures.

A potential unintended consequence of this recommendation could be a reduction in effort or resource allocation toward EOC readiness as a result of relaxing the regulatory framework that comes with NIMS and ICS. To combat this, alternative requirements to NIMS compliance must be developed. Rather than validating NIMS compliance, each jurisdiction must be required to submit an EOC plan that details the EOC's organizational structure, policies, and operational procedures, including activation and information-sharing mechanisms. An important part of this effort includes removing the contingency that grant funding is dependent on NIMS compliance; the EOC plan should serve as substitute.

3. Prioritize Local Government's Incorporation of the Private Sector in All Phases of Emergency Management

As a field, emergency management needs to shift its focus to incorporate the private sector in planning, training, and exercise processes prior to an incident. Since the release of the "2017 Hurricane Season FEMA After-Action Report," the agency's narrative for incorporating, and even relying on, the private sector has widened steadily.[120] The federal government realized it cannot respond to a catastrophic crisis without the private sector's support. This mindset must be adopted at the local government level. In the same way many local emergency management departments engage in community-based preparedness efforts, they need to develop equivalent curriculum for businesses to incorporate the private sector into all phases of emergency management.

The value of developing a preparedness curriculum for the private sector is twofold. First, when businesses are prepared for a crisis they free up critical government resources and can contribute to response efforts rather than draw down limited resources. Second, outreach efforts to engage the private sector start a dialogue about emergency

[120] FEMA, *2017 Hurricane Season FEMA After-Action Report* (Washington, DC: Department of Homeland Security, 2018), https://www.fema.gov/media-library-data/1531743865541-d16794d43d3082544435e1471da07880/2017FEMAHurricaneAAR.pdf.

management's mission space, how the private sector may be called on, and how they can best help. Ultimately, the private sector must be as engaged as every traditional emergency management partner and must be incorporated into emergency management.

D. FUTURE RESEARCH

A legitimate criticism of the recommendations provided in this thesis is that the lack of standardization they suggest will hinder accountability for readiness at the local government level. Future research should focus on developing and implementing performance metrics for local government EOCs. Currently this is achieved, in part, by NIMS training participation levels. The proposed recommendations, which eliminate the use of NIMS when appropriate, would eliminate a major metric for participation and compliance. To sustain a compliance infrastructure, further research should seek to develop national standards for readiness that extend beyond the response phase of emergency operations. Standardizing emergency management functions that are increasingly becoming hallmarks of the field, like long-term recovery, family assistance operations, and cyber-incident response, and determining how to use these plans as a metric for readiness and accountability deserves additional consideration and research.

E. POSTSCRIPT

As a relatively young professional field, emergency management has reached a major crisis of character. Are emergency managers first responders or not? Because the emergency management profession has aligned itself so closely with first responders, it has decreased opportunities for collaboration with other critical stakeholders. Some of this has been forced upon local governments by the extensive federal doctrine issued by FEMA and grant funding tied to NIMS compliance, and some of it is cultural. As the nation faces new and novel threats and hazards, like those from a catastrophic attack against critical infrastructure, emergency management must reevaluate its position.

Strong relationships with stakeholders are a hallmark of emergency management, and it is time to cast a wider net. To bring the right people to the table, we need to lower the knowledge barrier for entry into the emergency management sphere. The relationships that emergency managers have with partners will determine if they succeed or fail, and the

field must to do more to incorporate partners into its response operations. NIMS must be replaced with a set of common-sense policies that reflect the responding jurisdiction's unique needs and incorporate a wide range of second- and third-tier stakeholders. As emergency managers consider new threats and hazards of an increasingly wicked nature, it is critical to grow the spectrum of potential partners in incident response.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SOTHIRSTY TABLETOP EXERCISE

The document provided in this appendix has been built from the HSEEP Sitution Manual template available at https://preptoolkit.fema.gov/web/hseep-resources/conduct. The template, a commonly used tool during the conduct of emergency management exercises, is in compliance with HSEEP formatting and required content. The template has been populated by the author based on the scenario developed for this thesis.

SoThirsty Exercise

Situation Manual

This Situation Manual (SitMan) provides exercise participants with all the necessary tools for their roles in the exercise. Some exercise material is intended for the exclusive use of exercise planners, facilitators, and evaluators, but players may view other materials that are necessary to their performance. All exercise participants may view the SitMan.

EXERCISE OVERVIEW

Exercise Name	SoThirsy Exercise
Exercise Dates	[Indicate the start and end dates of the exercise]
Scope	This exercise is a table top exercise, planned for 5 hours at [exercise location]. Exercise play is limited to [exercise parameters].
Mission Area(s)	Response
Core Capabilities	Planning, Operational Coordination, Logistics and Supply Chain Management, Situational Assessment
Objectives	Identify needed policies and procedures for local government EOCs to incorporate government departments and private sector organizations not regularly involved in EOC operations in to response operations,
Threat or Hazard	Cyber-based critical infrastructure outage
Scenario	A catastrophic water outage has impacted several local government jurisdictions and is anticipated to occur for at least seven days.
Sponsor	[Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable]
Participating Organizations	Participating local government organizations should include: emergency management, social services, transportation, public works, and jurisdictional attorneys, at a minimum. Additional participating organizations should include: non-profits, local hospitals, and a diverse range of private sector stakeholders.
Point of Contact	[Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor)]

GENERAL INFORMATION

Exercise Objectives and Core Capabilities

The following exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s). The objectives and aligned core capabilities are guided by elected and appointed officials and selected by the Exercise Planning Team.

Exercise Objectives	Core Capability
Planning	Conduct a systematic process engaging the whole community as appropriate in the development of executable strategic, operational, and/or tactical-level approaches to meet defined objectives.
Operational Coordination	Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.
Logistics and Supply Chain Management	Deliver essential commodities, equipment, and services in support of impacted communities and survivors, to include emergency power and fuel support, as well as the coordination of access to community staples. Synchronize logistics capabilities and enable the restoration of impacted supply chains.
Situational Assessment	Provide all decision makers with decision-relevant information regarding the nature and extent of the hazard, any cascading effects, and the status of the response.

Table 1. Exercise Objectives and Associated Core Capabilities

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Players:** Players are personnel who have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
- **Observers:** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
- **Facilitators:** Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
- **Evaluators:** Evaluators are assigned to observe and document certain objectives during the exercise. Their primary role is to document player discussions, including how and if those discussions conform to plans, polices, and procedures.

Exercise Structure

Players will participate in the following 3 modules:

- Module 1: EOC Activation and Private Sector Integration

- Module 2: Developing a Common Operating Picture
- Module 3: Resource Sharing During an Incident

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in functional group discussions of appropriate response issues. For this exercise, the functional groups are as follows:

- Emergency Management Department
- Non-Public Safety Government Departments
- Private Sector Stakeholders
- Non-Profit Stakeholders

After these functional group discussions, participants will engage in a moderated plenary discussion in which a spokesperson from each group will present a synopsis of the group's actions, based on the scenario.

Exercise Guidelines

- This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected.
- Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
- Decisions are not precedent setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
- Issue identification is not as valuable as suggestions and recommended actions that could improve response efforts. Problem-solving efforts should be the focus.

Exercise Assumptions and Artificialities

In any exercise, assumptions and artificialities may be necessary to complete play in the time allotted and/or account for logistical limitations. Exercise participants should accept that assumptions and artificialities are inherent in any exercise, and should not allow these considerations to negatively impact their participation. During this exercise, the following apply:

- The exercise is conducted in a no-fault learning environment wherein capabilities, plans, systems, and processes will be evaluated.
- The exercise scenario is plausible, and events occur as they are presented.
- All players receive information at the same time.

Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned capabilities, capability targets, and critical tasks, which are documented in Exercise Evaluation Guides (EEGs). Evaluators have EEGs for each of their assigned areas. Additionally, players will be asked to complete participant feedback forms. These documents, coupled with facilitator observations and notes, will be used to evaluate the exercise and compile the After-Action Report (AAR).

MODULE 1: DEVELOPING A COMMON OPERATING PICTURE

Scenario

June, 2, 2022: 2:15 PM

On a warm Tuesday in June 2022, a disgruntled contractor working for the utility providing drinking water to the [XXXX] Region accesses an unattended water pumping station. He releases the SoThirsty virus into the utility's industrial control systems before departing for headquarters to turn in his letter of resignation. Over the course of several weeks, the SoThirsty virus reduces the amount of chlorine released into the drinking water system incrementally. Since inspections on the water's conformity with standards are automated by industrial control systems, the chlorine level decrease goes unnoticed by operators. The chemical formula used to prepare water to meet drinking standards is out of balance. Chlorine treatment is the foundation of preventing waterborne diseases that cause illness or even death like e. coli or cryptosporidium.

June, 30, 2022: 8:00 AM

After four weeks, reports of strange smelling drinking water trickle into the utility customer service line. Across the region, Emergency Departments are filling with patients with flu-like symptoms, some severe. Only when utility workers notice algae growing on water tanks are purity checks performed manually and the impacts of the contamination confirmed. Upon this realization the utility shuts down distribution until proper water treatment processes can be validated to protect people from getting sick.

June, 30, 2022: 10:00 AM

Without water pressure, wastewater discharge services cease, causing sewage to back up within homes, office buildings, restaurants, hotels, and hospitals in the affected locations. Local hospitals experience a surge in patients displaying severe symptoms of e. coli or cryptosporidium illness. Due to a lack of water pressure flights in and out of the local airport are suspended, without water pressure fire suppression systems cannot be operated to meet federal aviation standards. During this time frame, the public expects service to be restored and potable water to flow from faucets. Requests for potable water have been made to the state level emergency management department.

Key Issues

- Water service has been discontinued throughout the region for an unknown amount of time. As a result, sewage is backing up into homes and businesses causing closures.
- The water outage is widespread throughout the region but impacts specific to each jurisdiction are unknown.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 1. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Emergency Management Department

1. Who are the primary stakeholders needed to develop a comprehensive common operating picture? To include, non-profits, private sector entities, and non-traditional government partners?
2. How would you adjust your information collection practices to gather a comprehensive common operating picture?
3. How would you activate a Business Emergency Operations Center (or equivalent)?

Non-Public Safety Government Departments

1. If you are experiencing an impact from the water outage, who would you report that to in the government?
2. Who would you contact to receive status updates about the water outage?
3. What types of information would help you make operational decision for your organizations during the water outage?

Private Sector Partners

1. If you are experiencing an impact from the water outage, who would you report that to in the government? i.e. the Public Health Department, etc.?
2. Who would you contact to receive status updates about the water outage?
3. What types of information would help you make operational decision for your organizations during the water outage?

Non-Profit Partners

1. If you are experiencing an impact from the water outage, who would you report that to in the government? i.e. the Public Health Department, etc.?
2. Who would you contact to receive status updates about the water outage?
3. What types of information would help you make operational decision for your organizations during the water outage?

MODULE 2: EOC ACTIVATION AND STAKEHOLDER INTEGRATION

Scenario

June, 30, 2022: 4:00 PM

Local governments are issuing Declarations of Emergency and Emergency Management Departments are activating their EOCs. Immediately after the first reports of the water outage are released sales of potable water surge in the impacted region. The news media issue reports of looting for potable water though no evidence is produced. Establishments that still have water in stock request law enforcement support to quell disputes that store managers worry may grow into violence.

Without water pressure sanitation systems fail, leaving sewage backing up into homes and businesses. Those with financial means travel outside the impacted region for medical treatment and to access drinking water and properly functioning sanitation systems.

The water outage prevents hospitals and medical facilities from sanitizing instruments and surfaces, increasing the spread of bacteria. Hospitals throughout the region suspend operations and transfer patients out of the affected area despite the surge in demand from patients suffering from exposure to cryptosporidium and e. coli. Due to the water outage Public Health Inspectors close restaurants. The lack of water makes it impossible to sanitize dishes and utensils, cooking tools, or perishables. Per regulation, Fire Marshall's close schools and office buildings due to the lack of fire suppression and sanitation systems.

Local EOCs have been told by state level emergency management departments that it will take 72 hours for potable water supplies to arrive.

Key Issues

- Water has not been restored at this time. Hospitals, restaurants, hotels, and office buildings are closing indefinitely.
- Emergency Management officials have identified and engaged key stakeholders needed to support response operations. The majority of them are have never been to an EOC before and are unfamiliar with NIMS policies and protocols.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 2. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Emergency Management Department

1. What challenges will your partners face integrating in to EOC operations?
2. What steps can you take ahead of time to ease this?
3. How would you identify and contact necessary partners as you identify them?

Non-Public Safety Government Departments

1. If your organization can contribute resources (supplies, personnel, etc.) to response efforts how would you share them? Would you contact another government agency or non-profit? Would you utilize your own connections to distribute goods or assist individuals impacts by the outage?
2. What questions do you have about how an EOC operates and what your role is?
3. What EOC practices could be implemented to facilitate your integration?

Private Sector Partners

1. If your organization can contribute resources (supplies, personnel, etc.) to response efforts how would you share them? Would you contact a government agency or non-profit? Would you utilize your own connections to distribute goods or assist individuals impacts by the outage?
2. What questions do you have about how an EOC operates and what your role is?
3. What EOC practices could be implemented to facilitate your integration?

Non-Profit Partners

1. If your organization can contribute resources (supplies, personnel, etc.) to response efforts how would you share them? Would you contact a government agency or other non-profit? Would you utilize your own connections to distribute goods or assist individuals impacts by the outage?
2. What questions do you have about how an EOC operates and what your role is?
3. What EOC practices could be implemented to facilitate your integration?

MODULE 3: RESOURCE SHARING DURING AN INCIDENT

Scenario

July, 4, 2022: 10:00 AM

The water outage continues. Without water, heating ventilation, and air conditioning (HVAC) systems cannot operate. Every hotel room in the impacted area is vacant and restaurants are closed. Close to 100% of shift workers have been laid off until water is restored. As a result of school closures due to the water outage, students who rely on low and no cost lunch and breakfast programs go without meals.

A spontaneous evacuation of people out of the impacted region triggered a run on gasoline. Stations are rushing to restock fuel but the demand exceeds the supply chain's capacity. The exodus reduced the demand for goods significantly and grocery and convenience stores close indefinitely. As a result, regular donations to food banks are suspended, making the impacts of the water outage disproportionately severe for those who rely on social support services. Many members of the same population rely on shift work from hospitality industry jobs and have been laid off due to the hotels and restaurant closures. Vulnerable populations have been thrust from a difficult situation into a dire one.

The repercussions of the water outage have permeated the nation. The store closures have halted the flow of goods into the region and caused delays across the country. Major corporations are reimagining their supply lines to avoid the impacted region and work to develop strategies to store the unsold goods. Freight that would normally travel by truck through the region is diverted impacting business along the major transportation corridors.

Key Issues

- Individuals with financial resources are fleeing the impacted region, leaving behind those most in need of assistance.
- The impacts of the water outage have extended beyond the immediately effected region and are causing significant disruption.

Questions

Based on the information provided, participate in the discussion concerning the issues raised in Module 3. Identify any critical issues, decisions, requirements, or questions that should be addressed at this time.

The following questions are provided as suggested subjects that you may wish to address as the discussion progresses. These questions are not meant to constitute a definitive list of concerns to be addressed, nor is there a requirement to address every question.

Emergency Management Department

1. How would you like to receive information from other jurisdictions? How would you share information?

2. What policies and procedures can be put in place throughout the region prior to an incident occurring to facilitate coordination?
3. What legal or statutory regulations prohibit you from sharing resources or collaborating with the private sector and non-profit partners?

Non-Public Safety Government Departments

1. Does your organization participate in any regional or multi-jurisdictional groups or organizations that could be relevant to emergency response operations?
2. What legal or statutory regulations prohibit you from sharing resources or collaborating with the private sector and non-profit partners?
3. Does your organization have policies for suspending normal procurement or contractual requirements during an emergency?

Private Sector Partners

1. Does your organization participate in any regional or multi-jurisdictional groups or organizations that could be relevant to emergency response operations?
2. What legal or statutory regulations prohibit you from sharing resources or collaborating with the private sector and non-profit partners?
3. Does your organization have policies for suspending normal procurement or contractual requirements during an emergency?

Non-Profit Partners

1. Does your organization participate in any regional or multi-jurisdictional groups or organizations that could be relevant to emergency response operations?
2. What legal or statutory regulations prohibit you from sharing resources or collaborating with the private sector and non-profit partners?
3. Does your organization have policies for suspending normal procurement or contractual requirements during an emergency?

THIS PAGE INTENTIONALLYL EFT BLANK

APPENDIX B. COMPILED SOTHIRSTY SCENARIO

This appendix shows the cumulative scenario moves presented throughout the thesis, along with their worst- and best-case impacts.

A. SCENARIO MOVE 0

SoThirsty Scenario Move 0 (00:01–00:30 Minutes)

On a warm day in June 2022, a disgruntled contractor working for the utility that provides drinking water to the National Capital Region (approx. 6 million people*) accesses an unattended water pumping station. The contractor releases the SoThirsty virus into the utility's industrial control systems, then departs for headquarters to turn in his letter of resignation.

Over the course of several weeks, the SoThirsty virus incrementally reduces the amount of chlorine released into the drinking water system. Chlorine treatment is the foundation of preventing waterborne diseases that cause illness or even death, like e. coli or cryptosporidium.** Since inspections on the water's conformity with standards are automated by industrial control systems, the changes in chlorine level go unnoticed by operators. The chemical formula used to prepare water to meet drinking standards is out of balance.

After four weeks, reports of strange-smelling drinking water trickle into the utility customer service line. Across the region, emergency departments are filling with patients with flu-like symptoms, some severe.*** Only when workers notice algae growing on water tanks are purity checks performed manually and the impacts of the contamination confirmed.

Upon this realization, the utility shuts down distribution until proper water treatment processes can be validated, to protect people from getting sick. Without water pressure, wastewater discharge services cease, causing sewage to back up in homes, office buildings, restaurants, hotels, and hospitals in the affected locations. Local hospitals experience a surge in patients with severe symptoms of e. coli and cryptosporidium illness. Due to a lack of water pressure, flights in and out of Reagan National Airport are suspended; without water pressure, fire suppression systems cannot be operated to meet federal aviation standards. During this time, the public expects service to be restored and potable water to flow from faucets.

At 06:00 hours after water distribution ceases, emergency declarations from impacted local governments start to be issued. Local governments open their emergency operations centers (EOCs) to manage the impacts of the water outage.

* Jeff Clabaugh, "Washington Metro Population Climbs to 6.2 Million," WTOP, March 22, 2018, https://wtop.com/business-finance/2018/03/washington-metro-population-climbs-to-6-2-million/.

** Chlorine Chemistry Council, "Drinking Water Chlorination: A Review of Disinfection Practices and Issues" (report, Chlorine Chemistry Council, 2003), 2, https://waterandhealth.org/wp-content/uploads/2017/04/dwwp.pdf.

*** Chlorine Chemistry Council.

B. SCENARIO MOVE 1

SoThirsty Scenario Move 1 (00:30–24:00 Hours)

Immediately after the first reports of the water outage, sales of potable water surge in the impacted region. The news media issue reports of looting for potable water, though no evidence is produced. Establishments that still have water in stock request law enforcement support to quell disputes that store managers worry may grow into violence. Without water pressure, sanitation systems fail, leaving sewage backing up into homes and businesses. Those with the financial means travel outside the impacted region for medical treatment and to access drinking water and sanitation systems.

The water outage prevents hospitals and medical facilities from sanitizing instruments and surfaces, increasing the spread of bacteria. Hospitals throughout the region suspend operations and transfer patients out of the affected area, despite the surge in demand from patients suffering from exposure to e. coli and cryptosporidium. Due to the water outage, public health inspectors close restaurants; it is impossible to sanitize dishes and utensils, cooking tools, or perishables. Per regulation, fire marshals close schools and office buildings due to the lack of fire suppression and sanitation systems.

Reagan National Airport suspends operations once water pressure dwindles. Per regulation, without the mandated fire suppression capability, in-bound and out-bound flights must be halted. Immediately the air traffic infrastructure across the nation is plunged into disarray. Dozens of flights already in the air must be redirected to other airports. Future flights are delayed at first, only to be canceled. Thousands of passengers trying to get to Washington, DC, are stranded, and those whose planes or crew were coming from Washington, DC, are left grounded. By hour 24, the financial impacts incurred by airlines are significant, and they are rushing to upstaff their customer service support teams to mitigate damage to their brands due to customer outrage.

Validated information is slow to emerge from the water utility, and rumors are running wild both within the local government EOC and among the public. The public is calling 9-1-1 for more information about the incident, slowing response times to incidents threatening life safety. Major third-tier stakeholders and the federal government issue incorrect service restoration times based on news media reports, causing mass confusion and weakening the public's trust in the government.

Worst-Case Scenario Impacts: Scenario Move 1

- Across the impacted region, EOCs use National Incident Management System (NIMS) and Incident Command System (ICS) processes to conduct operations. The operational battle rhythm and policies specific to EOCs are challenging for second- and third-tier responders to understand. Many have never been in an EOC and cannot determine what is expected of them or how to best support operations. Incident response operations slow considerably while emergency management staff members conduct just-in-time training. Second-tier responders are unfamiliar with the ICS forms and defer to their internal reporting systems, which are not standardized across stakeholders. The lack of standardization between the report formats takes significant effort to reconcile by EOC leadership.

- No mechanism exists to collect situational updates from the third-tier stakeholders, and limited personnel are assigned to this task.* There is no visibility on mid- and long-term issues that may arise, limiting the effectiveness of response operations. Without gathering situational awareness from third-tier stakeholders, EOC leaders are operating without a complete common operating picture. As a result, guidance issued by the responding jurisdictions is inaccurate or irrelevant, increasing the public's frustration.

- Third-tier representatives with resources to share do not know who to contact to participate in response operations, and grow frustrated.

- Requests are made to state-level emergency management organizations to procure potable water. These requests can be approved quickly, but there are delays in receiving the products. As local governments look to other solutions for rapid procurement, local government attorneys become significant players in expediting procurement of essential goods. Unfortunately, there are substantial legal barriers for collaboration that local governments and third-tier stakeholders must overcome. Without a way to expedite procurement of needed commodities, the willing and able vendors cannot assist with response operations through the government incident response framework.

* The Liaison Officer is the official NIMS/ICS position that supports engagement of nongovernmental stakeholders. FEMA, *National Incident Management System*, 3rd ed. (Washington, DC: Department of Homeland Security, 2017), https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf.

Best-Case Scenario Impacts: Scenario Move 1

- The policies and procedures used to operate EOCs reflect common sense, and novice responders are easy to incorporate. When second- and third-tier responders arrive at EOCs, they can quickly start contributing to developing a common operating picture. Throughout the EOC, visual prompts reinforce the common-sense structures used to organize operations.

- Local government attorneys have minimal challenges interfacing with the players at the EOC due to the easy-to-understand operational framework. The coordination of crisis procurement processes results in reduced bureaucratic red tape and expedites the procurement of critical resources.

- Some third-tier stakeholders are severely impacted by the incident; others are major players in response operations. Those with critical resources to share are eager to support incident response operations. When EOCs reach full operational status, virtual business emergency operations centers (BEOCs) are activated. The virtual format allows for a secure exchange between the EOC and third-tier stakeholders on issues specific to the private sector. Third-tier stakeholders quickly learn that the BEOC is the best avenue for accessing information about the incident and to facilitate resource sharing with other third-tier stakeholders and the EOC. Access to the BEOC is easily granted: interested parties can request access via the Office of Emergency Management's website.

C. SCENARIO MOVE 2

SoThirsty Scenario Move 2 (72:00 Hours)

The water outage continues. Without drinking water, functioning sanitation systems, or medical services, those with the ability to do so are fleeing the region. The mass migration has triggered a run on gasoline. Stations are rushing to restock fuel but the demand exceeds the supply chain's capacity.

The news media has released more reports of looting, and smartphone video footage shows people breaking into grocery stores looking for bottled water. Reports state that some stores in the impacted region are selling a case of bottled water for over $75. The most vulnerable members of society, those without the resources to leave the impacted region, are still without access to drinking water. Emergency management officials are still securing potable water resources for those who cannot travel to access water.

Heating, ventilation, and air conditioning systems cannot operate without water, and plumbing systems stop working. As a result, office buildings close, displacing almost 1.3 million employees supporting the federal government mission from their worksites.* Some organizations direct staff to telework. Network servers in impacted office buildings must be powered down to avoid overheating, limiting the ability to conduct day-to-day operations via telework. Small businesses that rely on foot traffic around office buildings worry about their businesses' viability during a prolonged period of decreased customers.

Hotels in the impacted area are vacant, including 33,000 rooms in Washington, DC.** Hotels and restaurants are closed and have laid off all shift workers until water is restored. As a result of school closures due to the water outage, students who rely on low- and no-cost lunch and breakfast programs go without meals.

* Jeff Clabaugh, "Exactly How Many Washingtonians Work for the Federal Government?" WTOP, February 19, 2018, https://wtop.com/business-finance/2018/02/exactly-many-washingtonians-work-federal-government/.

** "Washington, DC Visitation and Impact (2017)," Destination DC, accessed February 25, 2020, https://washington-org.s3.amazonaws.com/s3fs-public/2017_visitor_fact_sheet.pdf.

Worst-Case Scenario Impacts: Scenario Move 2

- Third-tier stakeholders want to leverage their resources but have not been able to find the appropriate contact within the EOC. Instead, these actors create their own water distribution systems. Swarms of people quickly overwhelm distributors, creating a fertile ground for riots to develop. Urgent 9-1-1 calls requesting law enforcement support spike and divert resources from other critical law enforcement activities.

- Without a mechanism to gather information from third-tier stakeholders, to include nonprofit organizations, incident responders cannot anticipate the need to provide supplemental meals to students who rely on school meal programs until the situation has already grown into a crisis.

- Though there is a great need to facilitate refueling of gas stations, there is no infrastructure in place to begin a conversation with the necessary stakeholders for status updates and other situational awareness. Many station owners would gladly report the volume of customers they are seeing and keep EOC leadership up to date with shipment delivery times, but they are unaware there is a need for this information.

- Overly optimistic restoration times issued by the government frustrate third-tier stakeholders who would have otherwise acted to mitigate the impacts of the water outage on their business. As a result, representatives from corporations in the impacted area reach out to politicians to ask for more comprehensive updates. Meeting each of these requests detracts from EOC leadership's ability to focus on response operations, further delaying the development of a comprehensive common operating picture.

- Second-tier stakeholders in the EOC are frustrated by NIMS regulations. The operational tempo and ICS forms seem to be in a foreign language.

Best-Case Scenario Impacts: Scenario Move 2

- As it becomes apparent that an unofficial evacuation is occurring, EOC leadership reaches out to the business community via the BEOC to identify any known leaders within the convenience and fuel retailing community. Within hours the EOC has a few contacts who can provide status updates from their networks, greatly contributing to a common operating picture. Information is easily exchanged via the BEOC.
- Third-tier stakeholders with extensive supply chain networks access bulk drinking water supplies and connect with response personnel via the BEOC.
- Second- and third-tier community-based stakeholders have checked in with the populations they serve and their synthesized information has been incorporated into the common operating picture. Several issues are identified as they are forming, allowing responders to take action and mitigate the impacts before they escalate. As a result of these community-based organizations' incorporation into incident response operations, the EOC coordinates with social services and third-tier stakeholders to organize free breakfast and lunch services for students who qualify, as schools are not in session.
- As new nontraditional responders cycle into the EOC, the easy-to-understand procedures prevent a need for just-in-time training.

D. SCENARIO MOVE 3

SoThirsty Scenario Move 3 (Day 7)

Water service has not been restored at this time. Office buildings, hotels, and restaurants remain closed. Much of the population in the impacted area has evacuated the region. The exodus has reduced the demand for goods significantly, and grocery and convenience stores close indefinitely. As a result, regular donations to food banks are suspended, making the impacts of the water outage disproportionately severe for those who rely on social support services. Many members of the same population rely on shift work from hospitality industry jobs from which they have been laid off due to business closures. By day seven, vulnerable populations have been thrust from a difficult situation into a dire one.

The repercussions of the water outage have permeated the nation. The store closures have halted the flow of goods into the region and caused delays across the country. Major corporations are reimagining their supply lines to avoid the impacted region and work to develop strategies to store the unsold goods. Freight that would normally travel by truck through the Mid-Atlantic region is diverted, impacting business along the major transportation corridors.

Air traffic operations have been restructured to omit Reagan National Airport from routes. The planes and crews that comprised the almost 400 departures per day have been reallocated to other routes.*

The federal government has fully activated its continuity of operations plans and transitioned the majority of government functions to other parts of the country.

* "Washington, DC Visitation and Impact (2017)," Destination DC, accessed February 25, 2020, https://washington-org.s3.amazonaws.com/s3fs-public/2017_visitor_fact_sheet.pdf.

Worst-Case Scenario Impacts: Scenario Move 3

- Though there is a keen interest by third-tier stakeholders to contribute to response operations, the rigidity of NIMS goes against the business community's get-it-done ethos. When third-tier stakeholders are invited into the EOC or included in conference calls, the NIMS format is so foreign and technical that it is difficult to understand, and the formality seems unnecessary considering the urgency of the conditions.
- Pressure on politicians is mounting. Third-tier stakeholders are concerned about the government's capacity to effectively manage the incident and they are not hesitant to voice their frustrations. It is perceived that government operations have not considered the value the third-tier stakeholders bring to support incident response operations. EOC leadership diverts significant attention to respond to requests for information from politicians.
- EOC leadership is relying on man-on-the-street news reports from local business owners for specific updates on the business community's impacts.
- The need to provide breakfast and lunch to students who rely on school-based programs has grown to a crisis. Efforts at the EOC have shifted the focus from supporting the incident at large to prioritizing this issue.

Best-Case Scenario Impacts: Scenario Move 3

- With up-to-date and comprehensive information gathered from the BEOC about the extent of the impacts on third-tier stakeholders, EOC leadership assembles a more complete common operating picture.
- Second- and third-tier stakeholders see that, unless service industry employees can go back to work quickly, the cascading financial impacts may exceed the damage the water outage itself causes. Not only will the viability of businesses be threatened but employees who are at risk of missing a paycheck will need supplemental assistance. Recommendations are made to EOC leadership about the best courses of action to mitigate the cascading impacts.
- Local food banks are put on notice and are bracing for significantly higher-than-average customer demand and a decrease in available resources due to grocery store closures. With the advance warning, the organizations have time to use their connections to try to procure the needed resources.

LIST OF REFERENCES

Barnes, Julian. "Warning Lights Are Blinking Red." *New York Times*, July 13, 2018. https://www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html.

Bigley, Gregory, and Karlene Roberts. "The Incident Command System: High-Reliability Organizing for Complex and Volatile Task Environments." *Academy of Management Journal* 44, no. 6 (2017). https://doi.org/10.5465/3069401.

Blinder, Alan, and Nicole Perlroth. "A Cyberattack Hobbles Atlanta, and Security Experts Shudder." *New York Times*, March 27, 2018. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.

Buck, Dick, Joseph Trainor, and Benigno Aguirre. "A Critical Evaluation of the Incident Command System and NIMS." *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006). https://doi.org/10.2202/1547-7355.1252.

Burns, Shawn, David Della Volpe, Robin Babb, Nick Miller, and Gordon Muir. *War Gamers' Handbook: A Guide for Professional War Gamers*. Newport, RI: U.S. Naval War College. https://apps.dtic.mil/dtic/tr/fulltext/u2/1001766.pdf.

Chlorine Chemistry Council. "Drinking Water Chlorination: A Review of Disinfection Practices and Issues." Report, Chlorine Chemistry Council, 2003. https://waterandhealth.org/wp-content/uploads/2017/04/dwwp.pdf.

Clabaugh, Jeff. "Exactly How Many Washingtonians Work for the Federal Government?" WTOP, February 19, 2018. https://wtop.com/business-finance/2018/02/exactly-many-washingtonians-work-federal-government/.

———. "Washington Metro Population Climbs to 6.2 Million." WTOP, March 22, 2018. https://wtop.com/business-finance/2018/03/washington-metro-population-climbs-to-6-2-million/.

Cole, Dana. "The Incident Command System: A 25-Year Evaluation by California Practitioners." Research project, National Fire Academy, 2000. https://www.hsdl.org/?view&did=454470.

Department of Homeland Security. "National Incident Management System (NIMS) Fact Sheet." Accessed February 28, 2020. https://www.fema.gov/pdf/emergency/nims/NIMSFactSheet.pdf.

———. *National Preparedness Goal*, 2nd ed. Washington, DC: Department of Homeland Security, 2015. https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf.

Destination DC. "Washington, DC Visitation and Impact (2017)." Accessed February 25, 2020. https://washington-org.s3.amazonaws.com/s3fs-public/2017_visitor_fact_sheet.pdf.

Drabek, Thomas E., and Gerald J. Hoetmer (eds.). "Managing Disaster Response Operations." In *Emergency Management: Principles and Practice for Local Government*, 201–23. Washington, DC: International City Management Association, 1991.

Edzen, Svante. "Table-Top Exercises for Emergency Management: Tame Solutions for Wicked Problems." *47th Hawaii International Conference on System Sciences* (2014): 1978–1985. https://www.semanticscholar.org/paper/Table-Top-Exercises-for-Emergency-Management%3A-Tame-Edzen/2a4422445a3c25abec4744618aa115a5d9ca8c4c.

Eiten, Kimberly. "Baltimore Ransomware Attack: City Inches Closer to Normal Operations." CBS Baltimore, June 12, 2019. https://baltimore.cbslocal.com/2019/06/12/baltimore-ransomware-attack-inches-closer-to-normal/.

Federal Emergency Management Agency (FEMA). *2017 Hurricane Season FEMA After-Action Report*. Washington, DC: Department of Homeland Security, 2018.https://www.fema.gov/media-library-data/1531743865541-d16794d43d3082544435e1471da07880/2017FEMAHurricaneAAR.pdf.

———. "Community Lifelines." Accessed February 29, 2020. https://www.fema.gov/media-library-data/1544469177002-251a503b3717f0d6d483bae6169f4106/Revised_Community_Lifelines_Information_Sheet.pdf.

———. "Emergency Management: Definition, Vision, Mission, Principles." Accessed February 29, 2020. https://training.fema.gov/hiedu/docs/emprinciples/0907_176%20em%20principles12x18v2f%20johnson%20(w-o%20draft).pdf.

———. "Homeland Security Exercise and Evaluation Program, 2013." Report, Department of Homeland Security, 2013. https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

———. *National Incident Management System*, 3rd ed. Washington, DC: Department of Homeland Security, 2017. https://www.fema.gov/media-library-data/1508151197225-ced8c60378c3936adb92c1a3ee6f6564/FINAL_NIMS_2017.pdf.

Hambridge, Nicholas B., Arnold M. Howitt, and David W. Giles. "Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies." *Homeland Security Affairs* 13 (April 2017). https://www.hsaj.org/articles/13773.

Harrald, John R. "Agility and Discipline: Critical Success Factors for Disaster Response." *The Annals of the American Academy of Political and Social Science* 604 (March 2006): 256–72. https://www-jstor-org.libproxy.nps.edu/stable/25097791.

King County. "Regional Coordination Framework." Last updated July 25, 2019. https://www.kingcounty.gov/depts/emergency-management/emergency-management-professionals/regional-coordination-framework.aspx.

Lutz, Leslie D., and Michael K. Lindell. "Incident Command System as a Response Model within Emergency Operations Centers during Hurricane Rita." *Journal of Contingencies and Crisis Management* 16, no. 3 (September 2008): 122–34. https://doi.org/10.1111/j.1468-5973.2008.00541.x.

MARC. "Regional Coordination Guide." Accessed May 22, 2020. https://www.marc.org/Emergency-Services-9-1-1/MEMC/Other-Resources/Regional-Coordination-Guide

McGuire, Michael. "Collaborative Public Management: Assessing What We Know and How We Know It." *Public Administration Review* 66, no. s1 (December 2006): 33–43. https://doi.org/10.1111/j.1540-6210.2006.00664.x.

Metropolitan Washington Council of Governments. "Regional Emergency Coordination Plan." September 30, 2011. https://www.mwcog.org/file.aspx?A=l0xxarxHU0rCeawz0pCqkmn0rOQ1yOwK9ZoyvJUFCh4%3D.

Militello, Laura G., Emily S. Patterson, Lynn Bowman, and Robert Wears. "Information Flow during Crisis Management: Challenges to Coordination in the Emergency Operations Center." *Cognition, Technology and Work* 9 (2007): 25–31. https://doi.org/10.1007/s10111-006-0059-3.

Moynihan, Donald. "The Network Governance of Crisis Response: Case Studies of Incident Command Systems." *Journal of Public Administration Research and Theory* 19, no. 4 (October 2009): 895–915. https://www.jstor.org/stable/20627881.

National Infrastructure Advisory Council. *Water Sector Resilience: Final Report and Recommendations*. Washington, DC: Department of Homeland Security, 2016. https://www.dhs.gov/publication/niac-water-sector-resilience-final-report.

NBC News. “Baltimore’s 911 Emergency System Hit by Cyberattack.” March 28, 2018. https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. Washington, DC: Government Printing Office, 2004. https://www.9-11commission.gov/report/.

O’Brien, Geoff, Phil O’Keefe, Zaina Gadema, and Jon Swords. “Approaching Disaster Management through Social Learning.” *Disaster Prevention and Management* 19, no. 4 (2010): 498–508. https://doi-org.libproxy.nps.edu/10.1108/09653561011070402.

Perry, Ronald. “The Structure and Function of Community Emergency Operations Centres.” *Disaster Prevention and Management* 4, no. 5 (1995): 37–41. https://www.researchgate.net/publication/297655226_The_structure_and_function_of_community_emergency_operations_centres.

Quarantelli, E. L. “Ten Criteria For Evaluating The Management of Community Disasters.” *Disasters* 21, no. 1 (March 1997): 39–56. https://doi-org.libproxy.nps.edu/10.1111/1467-7717.00043.

Rufe, Roger, Carlton Moore, David Behler, John Cunningham, Larry Dietrick, Alexander Joves, David Moore, et al. *BP Deepwater Horizon Oil Spill Incident Specific Preparedness Review (ISPR): Final Report.* Washington, DC: U.S. Coast Guard, January 2011.

Ryan, Michael. “Planning in the Emergency Operations Center.” *Technological Forecasting and Social Change* 80, no. 9 (November 2013): 1725–31. https://doi.org/10.1016/j.techfore.2013.01.006.

Stubbart, Charles I. “Uncertainty, Complexity, Conflicts of Interest, Emotional Involvement, and the Quality of Crisis Thinking.” Faculty working paper, University of Illinois at Urbana-Champaign, September 1986. https://www.ideals.illinois.edu/bitstream/handle/2142/27634/uncertaintycompl1289stub.pdf?sequence=1&isAllowed=y.

Teeter, Andrew C. “On A Clear Day, You Can See ICS: The Dying Art of Incident Command and the Normal Accident of NIMS—A Policy Analysis.” Master’s thesis, Naval Postgraduate School, 2013. https://www.hsdl.org/?view&did=736338.

Tierney, Kathleen, and Joseph Trainor. “Networks and Resilience in the World Trade Center Disaster.” In *MCEER: Research Progress and Accomplishments 2003–2004*, 157–72. Buffalo, NY: University of Buffalo, 2004. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.537.5317&rep=rep1&type=pdf.

Waugh, William L. Jr., and Gregory Streib. “Collaboration and Leadership for Effective Emergency Management.” *Public Administration Review* 66, no. s1 (December 2006): 131–40. https://doi.org/10.1111/j.1540-6210.2006.00673.x.

White House. *National Preparedness*. Homeland Security Presidential Directive 8. Washington, DC: White House, 2003. https://www.hsdl.org/?view&did=441951.

Wong, Yuna Huh. “How Can Gaming Help test Your Theory?” *The RAND Blog*, May 18, 2016. https://www.rand.org/blog/2016/05/how-can-gaming-help-test-your-theory.html.

Wong, Yuna Huh, Sebastian Joon Bae, Elizabeth M. Bartels, and Benjamin Smith. *Next-Generation Wargaming for the U.S. Marine Corps: Recommended Courses of Action*. Santa Monica, CA: RAND, 2019. https://www.rand.org/pubs/research_reports/RR2227.html. Also available in print form.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California