JACK VOLTAIC 3.0

Cyber Research Report

Prepare | Prevent | Respond

Increasingly Connected, Ready to Respond

The Jack Voltaic (JV) Cyber Research Project is an innovative, bottom-up approach to critical infrastructure resilience that informs our understanding of existing cybersecurity capabilities and identifies gaps. JV 3.0 contributed to a repeatable framework cities and municipalities Nationwide can use to prepare. This report on JV 3.0 provides findings and recommendations for the military, federal agencies, and policy makers.

Lt. Col. Doug Fletcher | Lt. Col. Erica Mitchell | Maj. Erik Korn
Maj. Steve Whitham | Maj. Jason Hillman | Ron Yearwood
Clint Walker | Dr. Aryn Pyke | Dr. Gabriel Weaver | Brandon Pugh
Katherine Hutton | George Platsis | Timothy Klett | Ryan Hruska

ARMY CYBER INSTITUTE AT WEST POINT

FTI CONSULTING

CONTENTS

1. FOREWORD

Figure 1: Lt. Gen. Rhett A. Hernandez, USA (Retired)

During this period of strategic competition, nation-state competitors are attempting to gain strategic advantage by exploiting our Nation's critical infrastructure sectors. Secure and resilient critical infrastructure is essential for economic and national security. Every day we depend on and take the basic services provided by these sectors for granted. Given the interdependencies of these services, a risk to one can be a risk to all, and our networks are only as strong as their weakest links. To examine these interdependencies, one must look at cybersecurity and physical security from all perspectives. Critical infrastructure stakeholders—including the Department of Defense (DoD) and federal, state, municipal, and private sector partners—must work together to improve our Nation's resilience. Strong public-private partnerships at all levels are essential to security.

The Army Cyber Institute's (ACI's) Jack Voltaic (JV) series provides a bottom-up framework that enhances collaboration and creates a safe environment in which participants can assess, plan, and exercise their responses to physical, cyber, and informational attacks. This environment assists in identifying reporting requirements, information-sharing procedures, and incident declaration thresholds while providing a transparency that encourages a whole-of-community approach. For these reasons and others, the JV research project is a valuable tool in the mission to make the United States more cyber-resilient.

Compared to previous iterations, JV 3.0 was unique in several ways. Though it maintained focus on local-level participants, this iteration also explored how cyber disruptions on civilian critical infrastructure could impact the U.S. Army's ability to project forces. Additionally, JV 3.0 engaged multiple cities within the same region to gain a broader understanding of potential issues and explore diverse approaches to cyber incident response. Finally, the pandemic forced the ACI to transition from its typical on-site event to a distributed event; this new format allowed the ACI to explore its constant goal of providing a repeatable, low-cost, and scalable framework that is available to support local- to national-level exercises.

Finally, JV 3.0 would not have been possible without the ACI's partners' commitment and participation. Many thanks to the leaders who continued to support JV 3.0 while addressing the coronavirus disease 2019 (COVID-19) pandemic. Special thanks to the more than 200 individuals and 60 organizations who participated in September's JV 3.0 events virtually across the country. Your patience and persistence made this event possible and increased the Army's readiness.

The JV series remains important for the ACI because it provides insights and recommendations that are focused on increasing the Army's and our Nation's critical infrastructure resiliency. However, the ACI's work is made possible through strong public-private partnerships. The ACI is thankful for its partners and looks forward to continuing to collaborate with them.

— **Lt. Gen. Rhett A. Hernandez, USA (Retired)**
Cyber Chair, United States Military Academy

2. ACKNOWLEDGMENTS

In order to be successful, JV requires support from partners across government, academia, and industry. A team of West Point researchers and expert industry partners traveled to and from Charleston, South Carolina (SC), and Savannah, Georgia (GA), multiple times between 2019 and 2020, interviewing, designing, and planning JV 3.0 with hundreds of people and organizations from critical infrastructure sectors in those regions.

The authors of this report are grateful for the hospitality of our hosts: Mayor Van Johnson II, Mr. Patrick Monahan, Mr. Roy Minter, Mr. Derik Minard, Mr. Harry Campbell, and Mr. David Donnelly in the City of Savannah, GA; Mayor Allen Brown and Ms. Whitney Morris-Reed in the City of Hinesville, GA; Mayor John Tecklenburg, Mr. Wes Ratterre, and Mr. Ivan Torres in the City of Charleston, SC; and Mr. Eric DeMoura, Ms. Amanda Knight, and Mr. Jeffrey Jelks in the Town of Mount Pleasant, SC.

The authors appreciate the support and participation of the following state and federal government leaders: Maj. Gen. R. Van McCarty, Maj. Gen. Brad Owens, Col. David Gayle, and Lt. Col. William Medlin of the South Carolina National Guard; Chief Mark Keel, Special Agent Sean Fay, and Mr. Clint Walker of the SC Law Enforcement Division (SLED); the Honorable Wilbur Ross of the Department of Commerce; Mr. Ed Parkinson, Mr. Ed Horowitz, and Brig. Gen. Welton Chase, Jr., USA (Retired) of First Network Authority (FirstNet); Lt. Gen. Bradford J. Shwedo and Lt. Col. Ramon Morado of the Joint Staff J6; Lt. Gen. Stephen G. Fogarty, Maj. Gen. Robin L. Fontes, and Maj. Seth Hayden of U.S. Army Cyber Command; Lt. Gen. Laura Richardson and Lt. Col. Brett Bellizio of U.S. Army North; Maj. Gen. Antonio Aguto, Maj. Sean Frankum, and Chief Devon Spratling of the 3rd Infantry Division (3ID); Maj. Gen. Heidi J. Hoyle, Col. Michael Patrick, Lt. Col. Altwan Whitfield, Maj. Michael Biederman, Mr. Adam Gamez, Mr. John Murphy, Ms. Stacy Flippin, and Mr. John Trujillo of the Military Surface Deployment and Distribution Command (SDDC); Col. Brian L. Logan at Fort Stewart; Commander Wesley Sanders and Mrs. Aleksandra Scalco at Naval Information Warfare Command Atlantic; Mr. Jon Dollan and Mr. Rick Poland of Savannah River National Laboratory (SRNL); Dr. Mark Peters and Mr. Ryan Hruska of Idaho National Laboratory (INL); and Special Agent Jamie Nestor of the Federal Bureau of Investigation (FBI).

From academia, we would like to thank President Phil Susmann, Mr. John Kunelius, Dr. Kristen Pedersen, and Lt. Col. Tom Muehleisen, USA (Retired) of Norwich University Applied Research Institutes (NUARI); President Bob Caslen, Col. Mark Bieger, USA (Retired), Mr. Bill Kirkland, Mr. Chad Hardaway, Jr., and Mr. Jay Henderson of the University of South Carolina; Lt. Gen. Glenn M. Walters, USMC (Retired) and Dr. Shankar Banik of The Citadel; Dr. Kathy Love, Col. Pete Hoffman, USA (Retired), and Lt. Col. Scott Scheidt, USA (Retired) of Savannah Technical College (STC); Mr. Michael Shaffer and Col. Eric Toler, USA (Retired) of Augusta University and the Georgia Cyber Center (GCC); Dr. Gabriel Weaver of the University of Illinois at Urbana-Champaign (UIUC) Critical Infrastructure Resilience Institute (CIRI); and Dr. Charles Barry of the National Defense University.

The professionals from industry who contributed to our research and this report include Mr. John Klick, Mr. Ron Yearwood, Mr. Brian Stites, Mr. Jon Snyder, Ms. Sarah Mann, Mr. George Platsis, and Ms. Kristina Ecalnea of FTI Consulting; Ms. Jill Singer, Mr. Jason Porter, Mr. Bruce Westcott, and Ms. Barbara Galicia of AT&T; Dr. Annita Nerses, Mr. Matt Tighe, and Mr. Jason Winslow of Intrepid Networks; Maj. Sam Chanoski, USA (Retired) at Electricity Information Sharing and Analysis Center; Mr. Richard Nelson of SAIC; and Mr. Clement Danish of Blank Slate Solution.

3. INTRODUCTION: JACK VOLTAIC 3.0

3.1. Fictional Crisis

An international crisis in Europe prompts the President to order the rapid deployment of a brigade combat team as a show of force in support of U.S. allies. Forces are needed immediately, and any delay would further harm U.S. and North Atlantic Treaty Organization interests. As the United States begins to transport equipment from their forts to strategic ports, its adversaries begin a cyber assault on the domestic civilian-owned critical infrastructure that supports and facilitates such movement. The cyber assault starts with small, seemingly unconnected incidents: The port's gates begin having small malfunctions, several organizations experience minor issues with their administrative systems, and reports of a new phishing campaign surface. These small incidents soon give way to larger ones that cascade across critical infrastructure sectors and significantly tax local responders. While the public and private sectors respond to these multiple incidents, the brigade combat team's equipment is caught in the middle. The brigade combat team commander is closely monitoring the movement of the unit's equipment, but the commander realizes he or she must consider the possibility that the equipment may not arrive at the destination in time to effectively execute the current plan.

Adversarial competitors are increasingly leveraging cyber activities to gain strategic advantage over the United States, partner nations, and global industry using targeted espionage and attacks against all elements of critical infrastructure. For example, in February 2020, the United States Computer Emergency Readiness Team issued an advisory that a cyber threat actor had used a spear-phishing link to obtain access first to a natural gas company's information technology (IT) network, and then to its operational technology (OT) network. Next, the threat actor deployed commodity ransomware to encrypt data for impact on both networks. The company never lost control of its operations but still decided to implement a shutdown. Although the direct operational impact of the cyberattack was limited to one control facility, other facilities had to halt operations because of pipeline transmission dependencies, resulting in an operational shutdown of the entire pipeline that lasted about 2 days.[1]

The 2015 *Department of Defense Cyber Strategy* states, "In addition to DoD's own networks, a cyberattack on the critical infrastructure and key resources on which DoD relies for its operations could impact the U.S. military's ability to operate in a contingency."[2] The *Department of Defense Cyber Strategy 2018 Summary* states that the DoD "must be prepared to defend non-DoD-owned Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) networks and systems. [The DoD's] chief goal in maintaining an ability to defend DCI is to ensure the infrastructure's continued functionality and ability to support DoD objectives in a contested cyber environment."[3] The strategy document goes on to say that "the DoD will work with its interagency and private sector partners to reduce the risk that malicious cyber activity targeting U.S. critical infrastructure could have catastrophic or cascading consequences."[4]

[1] Alert (AA20-049A): Ransomware Impacting Pipeline Operations," United States Computer Emergency Readiness Team (website), updated October 24, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-049a.

[2] Department of Defense (DoD), *The Department of Defense Cyber Strategy* (Washington, DC: DoD, April 2015), 10.

[3] DoD, The *Department of Defense Cyber Strategy 2018 Summary* (Washington, DC: DoD, September 2018), 3.

[4] DoD, *Cyber Strategy 2018 Summary*, 5.

United States Cyber Command also highlights this critical guidance within its overarching imperatives. Imperative 5 outlines the need to "expand, deepen, and operationalize partnerships" in ways that "leverage the talents, expertise, and products in the private sector, other agencies, Services, allies, and academia."[5] The strategic importance of ensuring domestic critical infrastructure resilience is further reinforced by the *National Cyber Strategy of the United States of America's* pillar 1 ("Protect the American People, the Homeland, and the American Way of Life") in which "Secure Critical Infrastructure" is presented as a crucial component.[6] More recently, the second strategy layer ("Deny benefits") in the *Cyberspace Solarium Commission Final Report* emphasized this importance as well, stating, "National resilience efforts rely on the ability of the United States, in both the public and private sectors, to accurately identify, assess, and mitigate risk across all elements of critical infrastructure."[7]

The ACI's JV research project supports the 2015 and 2018 DoD Cyber Strategies while aligning with elements of the United States Cyber Command Vision, National Cyber Strategy, and *Cyberspace Solarium Commission Final Report's* layer-two strategic approach through the analysis of critical infrastructure resiliency, cyber incident response, and public-private partnerships. This concept grew from the energy sector's efforts to develop cyber mutual assistance, supporting sector coordination and resourced responses to major cyber incidents.[8] When an incident occurs, such as a natural disaster that causes a power outage, cyber mutual assistance ensures that assets and capabilities from across the Nation come together to provide response and recovery. JV expands this concept across multiple critical infrastructure sectors because the cyber domain innervates all sectors, creating various types of dependencies.

The JV research project enables the ACI to study incident response gaps alongside assembled partners to identify interdependencies among critical infrastructure and provide recommendations. JV provides an innovative, bottom-up approach to critical infrastructure resilience in two unique ways. Whereas most federal efforts to improve resiliency focus on regional or multistate emergency response, JV focuses on cities and municipalities where critical infrastructure and populations are most heavily concentrated. Furthermore, JV deviates from other cybersecurity and national preparedness exercises by building around areas of interest nominated by the participants. Although JV events include national-level capabilities and resources, they are conceptually driven by the concerns of the cities and their infrastructure partners. Through this approach, the ACI, the Army, and the DoD are able to gather unique insights about potential roles, dependencies, partners, and support requests, while cities are able to discover potential capability gaps and expand their critical infrastructure information-sharing networks before a potential disaster strikes.

[5] United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: United States Cyber Command, April 2018), 9.

[6] Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington, DC: The White House, September 2018), 8–10.

[7] U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report* (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020), 4

[8] Jonathon Monken et al., *Cyber Mutual Assistance Workshop Report* (Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute, 2018), https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_513596.pdf.

This bottom-up approach identifies key stakeholders and public-private partnerships, experimental design elements, governance hierarchies, exercise simulations, and relevant data collection points to elucidate critical insights into incident response gaps, vulnerabilities, as well as strengths.[9] The overarching research goals of the JV research series are:

- Identifying a repeatable and scalable framework usable by any city to rehearse responses to cyber events that affect multiple sectors and require coordinated responses.
- Providing a safe learning environment that enables participants to receive training on, assess, and gain exposure to and an appreciation for cyber, physical, and cyber-enabled physical incidents.
- Increasing communication between leadership and their technical teams and among organizations from different sectors.
- Improving information sharing and response coordination among municipalities; county, state, federal, and tribal organizations; industry; and the private sector.
- Providing DoD data, information, and feedback to validate planning assumptions and maintain readiness.

The ACI has conducted JV research for the past 4 years and, in that time, completed three experiments in the form of cyber exercises: JV 1.0 in New York City (NYC) from August 29 through 31, 2016; JV 2.0 in Houston from July 24 through 26, 2018; and JV 3.0 in Charleston on September 22, 2020, and in Savannah on September 24, 2020. In addition to these four events, the ACI held the JV 2.5 Cyber Workshop Series in the port cities of San Diego, Tacoma, San Francisco, Savannah, Charleston, Augusta, and Norfolk in summer 2019.

JV 3.0 leveraged the JV approach to allow the ACI to gain insight into how multiple levels of industry and government respond to a cyberattack against local, commercial, and federal critical infrastructure that supports Army force projection operations—specifically, critical infrastructure in port cities from which Army personnel and equipment would deploy in the case of a military conflict overseas.[10] In parallel with the Army's Defender 2020[11] force projection exercise, JV 3.0 examined and analyzed the ability of Charleston, South Carolina (SC), and Savannah, Georgia (GA)—two major port cities on the East Coast—to support force projection in the face of cyber aggression against all aspects of geographically aligned critical infrastructure.[12]

Originally planned as a 3-day event in April 2020 held simultaneously in these two port cities, the ACI decided to make JV 3.0 two single-day, virtual events—one for Charleston and one for Savannah—because of complications arising from the COVID-19 pandemic. Stakeholders from the two cities and states as well as public and private partners still participated in the virtual exercises using the Distributed Environment for Critical Infrastructure Decision-making Exercise (DECIDE®) platform and Microsoft Teams. Participants included representatives from the transportation, energy, emergency management, communications, information technology (IT), government facilities, and water/wastewater sectors.

[9] Erica Mitchell et al., *Jack Voltaic Critical Infrastructure and Public-Private Partnerships* (West Point, NY: United States Military Academy, July 18, 2019), 9.

[10] Mark Pomerleau, "How the Army Is Strengthening Cyber Cities," Fifth Domain, July 30, 2019, https://www.fifthdomain.com/dod/army/2019/07/30/how-the-army-is-strengthening-cyber-cities/.

[11] "DEFENDER-EUROPE 20," Supreme Headquarters Allied Powers Europe (website), n.d., https://shape.nato.int/defender-europe, accessed December 29, 2020.

[12] Shannon Vavra, "US Army Combines Fake Hacks, Natural Disaster Simulation to Test Municipal Responses," Cyberscoop, September 24, 2020, https://www.cyberscoop.com/army-savannah-charleston-cyber-test/.

When designing the scenario, the ACI and stakeholders based the scenario on real-life incidents to simulate a series of small, seemingly unrelated events instead of a single, catastrophic event. This "death by a thousand cuts" approach relied on the aggregation of all the events across the different sectors to create a situation that overcommitted local response resources in both cities. As a result, the scenario reinforced a whole-of-community approach to cyber incident response and critical infrastructure resiliency. It allowed participants to observe the responses of other participants and identify organizations and sectors with which they should communicate, thereby laying the groundwork for increased collaboration.

3.2. Origin and History of Jack Voltaic

3.2.1. Cyber Mutual Assistance Workshop (CMAW)

On April 8, 2016, the ACI conducted the initial phase of the JV research project, the Cyber Mutual Assistance Workshop (CMAW).[13] The workshop was led and facilitated by the ACI, the Electric Infrastructure Security Council, and Carnegie Mellon University. The CMAW provided an opportunity for practitioners and experts from the public and private sectors to examine cyber mutual assistance using a holistic approach and to share capabilities and issues concerning the energy sector.

During the CMAW, the ACI used a cyber exercise to examine mutual assistance from the angles of preparation, prevention, and response. The research objectives of the CMAW were:

- Define capability requirements for cyber;
- Discuss existing legal and operational frameworks;
- Develop partnerships;
- Develop a multisector exercise; and
- Define and plan a follow-on experiment to examine interdependencies among critical infrastructure sectors.

3.2.2. JV 1.0

JV 1.0 was a 2-day event in NYC in August 2016 that simulated a cyberspace attack impacting multiple sectors and exercised the city's ability to respond to such an attack.[14] JV 1.0 simulated a hypothetical cyber event involving a strategic, methodical attack occurring over 6 days. The first phase of the attack impacted the financial sector through a spear-phishing attack targeting a financial executive. In the second phase, the malicious actor targeted the energy sector by installing malicious software on a power company's network. The malware granted control of the company's power stations to the attacker, who used them as a pivot point to further exploit and compromise the city's transportation tunneling and signaling systems. This led to destructive malware targeting the city's water treatment plants.

JV 1.0 involved 25 organizations and 137 participants from six critical infrastructure sectors: financial services, emergency services, communications, healthcare, energy, and transportation systems. Developed with industry partner CITI, JV 1.0 examined interdependencies among critical infrastructure service providers in NYC. The ACI examined these interdependencies by assessing the performance of federal, state, and local governments, as well as private industry, in the event of a "Cyber Worst Day" scenario.

[13] Monken et al., *Cyber Mutual Assistance Workshop Report*.

[14] Army Cyber Institute (ACI), *Jack Voltaic Executive Summary* (West Point, NY: United States Military Academy, 2016); and Joseph W. Pfeifer, "Preparing for Cyber Incidents with Physical Effects," *The Cyber Defense Review* 3, no. 1 (2018): 26.

The main objective of JV 1.0 was to identify a framework in which to rehearse a city's coordinated responses to cyber incidents affecting multiple sectors. This exercise provided a venue in which participants could gain exposure, train players, and evaluate responses. The event produced the following findings:

- Cities still require their own ability to communicate up (to the state and federal levels) and across (within the city) to enable cyber preparation, prevention, and response.
- A municipality established cyber policy framework should inform and shape state and federal level polices.
- A municipality's escalation processes should include identified industry partners and leverage local, state, and federal information sharing centers.
- Municipalities need to work through the process of an outage and determine whether it is cyber related.
- Explore, develop, and maintain public/private partnerships at the local, state, and federal levels to enable an integrated and coordinated incident response.
- Municipalities need to integrate public affairs/communications into their response plans.

3.2.3. JV 2.0

A follow-up project to JV 1.0, JV 2.0 was a multi-sector, public-private cybersecurity research project that culminated in an exercise.[15] Occurring in July 2018, the 3-day event explored how a large city would respond to a simultaneous physical and cyberspace attack that could impact multiple critical infrastructure sectors. JV 2.0, which took place in Houston, explored the employment of the total Army force to defend the Nation in the face of a combined physical and cyberspace attack on a large U.S. port city as well as the cyber resiliency and readiness of Army-operated defense critical infrastructure to support military power projection and sustainment abroad from the port city. JV 2.0 centered on a hypothetical scenario in which a hurricane and cyberspace attack struck simultaneously in and around the Houston region. The event involved 44 organizations and 200 participants from eight critical infrastructure sectors.[16]

The intended outcome of JV 2.0 was to provide recommendations to U.S. Army Cyber Command (ARCYBER) on the development of strategies and procedures for defending large municipalities and critical infrastructure against cyberspace attacks and to develop Army cyber training objectives. Through JV 2.0, the ACI aimed to give state and regional civil officials a better understanding of how to leverage DoD and National Guard cyber capabilities to protect public and private critical infrastructure.

[15] Mitchell et al., *Jack Voltaic Critical Infrastructure*.

[16] Benjamin Freed, "Why Local Governments Should Lead Multi-Jurisdiction Disaster Response," StateScoop, April 23, 2019, https://statescoop.com/why-local-governments-should-lead-multi-jurisdiction-disaster-response/.

JV 2.0 enabled the establishment of public-private partnerships and a better understanding of the responses of private industry and government at multiple levels, facilitating the identification of gaps and the defense of key critical infrastructure cyber terrain.[17] With increases in the number of infrastructure sectors and Army stakeholders, JV 2.0 represented a more complex response environment than JV 1.0. The more complex set of responses built on the insights from JV 1.0 yet offered its own insights. Some of the lessons learned were:

- Political and civil agency leadership must view cyberspace as an operational domain involving adversaries who respond to contact, rather than viewing it in terms of static concepts of IT or cybersecurity architecture and policies.
- Cities should revisit their network monitoring of all OT / supervisory control and data acquisition (SCADA) systems in each sector to ensure that only secure communications between production networks and the open Internet are allowed.
- Though there are existing means for enabling cyber preparation, prevention, and responses, cities must have their own ability to communicate across (within the city), up (to the state and federal level and supporting sectors), and beyond (with commercially owned and operated critical infrastructure).
- Cyber policy development at the city/county level is needed to inform and shape state and federal policies.
- Cities and counties should engage in cyber exercises because they provide opportunities for local governments and private sector partners to experiment in a safe and trusted environment and collaboratively work through challenges, share best practices, and develop processes and procedures.

3.2.4. JV 2.5

In summer 2019, the ACI held the JV 2.5 Cyber Workshop Series in the port cities of San Diego, Tacoma, San Francisco, Savannah, Charleston, Augusta, and Norfolk.[18] The objectives of the cyber workshop series were to:

- Engage the owners of high-priority DoD critical infrastructure as well as municipality leaders on key relationships between commercial critical infrastructure and DoD critical missions;
- Disseminate information and educate public and private entities on the lessons learned from JV 2.0;
- Increase cyber awareness knowledge and provide information on cyber response option support; and
- Prepare for the JV 3.0 exercise.

[17] Natasha Cohen, *Cyber Incident Response and Resiliency in Cities: How Partnerships Can Be a Force Multiplier* (Washington, DC: New America, updated February 21, 2019).

[18] ACI, "Jack Voltaic 2.5 Cyber Workshop Series," ACI (website), 2019, https://cyber.army.mil/Portals/3/Documents/JackVoltaic/Jack%20Voltaic%202_5%20InfoSheet_v4.pdf?ver=2019-08-20-153840-620.

In support of these missions, AECOM and the ACI, in conjunction with the Department of Homeland Security (DHS) National Exercise Division, conducted a series of 1-day training workshops to share insights from JV 2.0 and discuss how similar efforts have the potential to strengthen the cyber resiliency of DoD missions. The workshops also helped to inform the scope of JV 3.0, which was still in its planning stages. Some of the key findings from the workshop series include:

- Cyber intrusions are considered an IT, not an operational, problem.
- The National Guard and the Reserves can serve as a very valuable DoD interface with local communities.
- There is a dearth of information sharing and dialogue between communities and DoD installations, but communities where DoD and community leaders work together can move faster to take the right next steps.
- At all levels, the operational planning community needs to emphasize and seamlessly integrate physical–cyber acknowledgment and response efforts that highlight IT- and OT-dependent systems.
- National-level exercises do not provide information on the readiness level of local communities, where incidents are occurring with increasing frequency.
- Partnerships, both public-private and public-public, are based on personal relationships in almost every location and need to be institutionalized.

Compounding observations from the JV research series that include more recent events, such as the JV 2.5 and JV 3.0 Legal and Policy Tabletop Exercise (TTX), include:

- Crisis management and remediation is personality driven.
- Individuals and organizations tend to lack experience with real cyber events and thus have difficulty visualizing second-, third-, and fourth-order effects; this inhibits a true understanding of interdependencies between organizations.
- Municipalities and private entities tend to lack cyber policies that are complete, executable, resourced, and accessible, whether specific frameworks or as annexes to existing crisis management policies, and too often treat cyber incidents as information technology concerns.
- Municipalities and organizations generally do not know what resources are available or who provides them during a cyber event; this result in hesitancy to declare a cyber incident.[19]
- Define and plan a follow-on experiment to examine interdependencies among critical infrastructure sectors.

[19] Robin L. Fontes et al., "Jack Voltaic®: Bolstering Critical Infrastructure Resilience," *The Cyber Defense Review* 5, no. 3 (2020): 50–53.

4. JACK VOLTAIC RESEARCH METHODOLOGY

4.1. Introduction

This chapter describes the development of the JV 3.0 research and experiment design, both as a discrete event and as part of a research series. JV 3.0 began with initial concept development by the ACI in May 2018, continued through execution in September 2020, and beyond into 2021 with data analysis and the publication of this report. Because JV is primarily municipality-focused and includes as many private partners as possible, planning and execution for this research relies on coordinating a coalition of willing participants. The value of the event depends on engaged participation from individuals and organizations with diverse perspectives and scopes of responsibility. Maintaining broad engagement and ensuring all participants received as much value from JV 3.0 as they provided via their participation are some of the greatest challenges of performing JV research. As such, it is important to note that this chapter provides a synthesis of design concepts, evolving requirements, and key decisions which resulted in the execution events. Additionally, this section will mainly be a summary of final decisions and designs; more details are provided in the appendices for those desiring to see a more complete description of the process.

This chapter begins with a detailed explanation of each of the five principal research objectives, including a full description, the motivation behind the objective, and how it was incorporated into the overall JV 3.0 research event. These objectives and the objectives of the participants are the unifying thread for all aspects of the JV development and execution process. The remaining sections of this chapter detail the main components of JV, the partner organizations that played key roles in supporting the development process, the participating organizations whose input was critical to JV research, the scenario that the team designed to draw out the JV research objectives, the data collection plan, and the planning time line.

4.2. Research Objectives

Preparation for the JV events centers around the five principal research objectives. This section provides a more detailed description of each objective, insight into the motivation behind the objective, and how the ACI planned to incorporate the objective into JV 3.0. The objectives of JV 3.0 were to:

- Examine the impact of a cyber event on Army force projection;
- Exercise the cities of Charleston and Savannah in emergency cyber incident response to ensure the provision of public services and safeguard critical infrastructure;
- Reinforce a whole-of-community approach in response to cyber incidents through sustained, multi-echelon partnerships across industry, academia, and government;
- Examine the coordination process for providing cyber protection capabilities in support of Defense Support to Civil Authorities (DSCA) requests; and
- Support the development of a repeatable and adaptable framework that allows a city to exercise its response to a multisector cyber event.

4.2.1. Examine the Impact of a Cyber Event on Army Force Projection

JV 2.0 highlighted the challenges ports face in preparing for and responding to a physical or cyberspace attack. This project identified gaps in understanding of cyber threats, service-level agreements, and overall cyber response procedures. As a result, one of the primary research objectives of JV 3.0 was to examine the impact of a cyber event on Army force projection.

To study cyber incident effects on Army force projection, the ACI wanted to explore in-transit visibility considerations, including the identity, status, and location of DoD units, unit cargo, passengers, and personal property; understand Army movement control systems that regulate movement according to command priorities and synchronize the distribution flow of land forces; and consider strategic mobility activities that can mitigate the effects of natural and man-made obstacles that could hinder freedom of maneuver. The ACI also wished to assess whether the DoD is prepared to execute appropriate contingencies, branches, and sequels if Charleston and/or Savannah are unable to support force projection as a result of a cyber incident.

To observe the effects of a cyberattack on the fort-to-port supply chain in the JV 3.0 exercise, the ACI incorporated Emotet and phishing attacks into the exercise scenario. Emotet infected ships and trains' cargo databases, and aggressive phishing attacks were directed at electricity and natural gas utilities. In addition, railway switching stations began to malfunction, resulting in further confusion and delays. To measure the effects of these disruptions on public and private sector operations and coordination, ACI data collectors observed the movement status of equipment; effects on military, civilian, and political decision making; effects on deployment; economic costs; vulnerabilities; response times; and second- and third-order effects on the mission (contingency planning).

4.2.2. Exercise the Cities of Charleston and Savannah

The focus of this research objective was to provide municipal organizations an opportunity to detect and respond to a cyber incident and assess their capability levels in that regard. Cities require the ability to provide adequate emergency cyber incident response to ensure the provision of public services and to safeguard commercial critical infrastructure. The ACI selected the cities of Charleston and Savannah due to their proximity to strategic ports that supported Defender 2020 and because both are in the same geographic region.

In the JV 3.0 experiment, the ACI wanted to identify and gauge cognitive, personal, and in-progress observations from the municipal emergency response perspective. In addition, the ACI wished to better enable municipal identification of potential gaps and threat vectors as well as response capabilities. The ultimate goal in this regard was to allow Savannah and Charleston to: (1) rehearse their capabilities and incident response plans; and (2) identify current gaps, critical infrastructure interdependencies, best practices, and existing resource allocations, thereby providing a common operating picture that informs the strengthening of cyber incident response mechanisms and bottom-up resiliency.

One of the intended effects of the scenario injects was to overcommit local public and private resources within the two port cities. Real-world examples were utilized to increase realism and believability.
The responsibilities of the ACI data collectors were to capture key municipal perspectives on potential individual, resource, and framework gaps in responding to a debilitating regional event. ACI data collectors collected survey data from municipal critical infrastructure executives on their municipalities' cyber incident response plans, capabilities, and resiliency; collected interview data to tell the story of

JV from the municipality level or higher; and gauged and measured the response efforts of municipal emergency response organizations during the various turns in the scenario.

4.2.3. Reinforce a Whole-of-Community-Approach

A whole-of-community approach is critical for improving the detection of and response to a cyber incident; in a digitally connected environment, the owners of compromised systems and devices put not only their own information and infrastructure at risk, but also the information and infrastructure of other organizations that depend on their services. Vulnerability to cyber disruption is a whole-of-community problem that requires multi-echelon, cooperative action by governmental entities as well as private industry if it is to be solved. JV's bottom-up approach focuses on a multi-echelon, cooperative approach to preparing communities that are highly likely to be targeted by malicious cyber actors.

The JV 3.0 scenario reinforced a whole-of-community approach to cyber incident response and critical infrastructure resiliency by allowing participants to observe the responses of other participants and to identify organizations and sectors with which they should communicate, thereby laying the groundwork for increased collaboration. The ACI wished to identify the municipal, state, federal, and industry partnerships, relationships, and collaborations that are necessary to support a whole-of-community approach to cyber incident response.

ACI data collectors focused on examining public-private partnerships; the internal capabilities, external support, and institutional knowledge of both government and industry; and the actions of participants from academia, including the involvement of institutional resources, federally funded research and development centers, nonprofit organizations, and think tanks.

4.2.4. Examine the Coordination Process for Providing Cyber Protection Capabilities in Support of DSCA

The focus of this research objective is to improve situational awareness of the DoD capabilities available to cities and states in the event they need support dealing with a cyber incident. DoD Directive 3025.18 establishes policy, assigns responsibilities, and provides guidance for the execution and oversight for DSCA, also referred to as civil support.[20] DSCA support is provided by U.S. federal military forces and DoD civilians, contract personnel, and component assets. This DSCA directive also authorizes emergency authority for the use of military force—such as the National Guard—once Title 32 of the U.S. Code is invoked and requested through the lead federal agency. DSCA support can only occur once civilian capabilities have been exhausted and support has been requested by civil authorities. DSCA is evaluated under "C.A.R.R.L.L.," which assesses the following aspects:

- Cost: Who pays, and what is the impact on the DoD's budget;
- Appropriateness: Whether the requested mission is in the department's interest to conduct;
- Risk: The overall safety of DoD forces;
- Readiness: Impact on the DoD's ability to perform its primary mission;
- Legality: Compliance with laws; and
- Lethality: Potential need for lethal force by or against DoD forces.

[20] William J. Lynn III, *Defense Support to Civil Authorities (DSCA)*, DoD Directive 3025.18 (Washington, DC: Office of the Secretary of Defense, December 29, 2010).

Regarding cyberattacks, cyber forces are not included in the execute order and not preprogrammed. Although governors and adjutant generals can provide cyber support to local governments and critical infrastructure using National Guardsmen in State Active Duty, all requests for cyber support under Title 10 go up to the level of the assistant secretary of defense as a result, after which a memorandum of understanding (MOU) or memorandum of agreement to send DoD support to the Cyber Protection Brigade is signed. All of this entails responding to physical impacts, assisting with halting the cyberattack and recovery efforts, and deploying forces (if required), all in coordination with other government agencies.

Though the DSCA process is well defined and understood at the local level, the process for requesting DoD support for cyber incidents through Defense Support to Cyber Incident Response (DSCIR) is not as clear. JV 3.0 sought to assist in clarifying and refining this process for all its participants through its Law and Policy TTX, an event that allows organizations to assess their cyber incident response plan, understand the composition and distribution of cyber assets across the state and federal government, and explore the authorities that govern the DSCIR process. Furthermore, the ACI tailored the scenario so that participants could exercise their incident command relationships, decision-making assistance, and information-sharing mechanisms.

4.2.5. Support the Development of a Repeatable and Adaptable Framework

This research objective, part of the JV research series strategy, is about making it as easy as possible for municipalities and private entities to conduct resiliency exercises while taking into account the conditions that make them unique. There are several processes publicly available for conducting exercise planning that include business, military, and even critical infrastructure. The ACI's goal is to go beyond providing a general process by eventually offering a platform that will assist in the creation of distributable documents, rapid scenario development, and conducting of events. JV 3.0 was designed to serve not only as a research experiment, but also as the first template for future JV events, regardless of whether they are led by the ACI. Additionally, the ACI is working on automating much of the process to reduce the time investment for exercise planners and assessors.

Because the ACI is a military entity, relationship building was a key aspect of coordinating a coalition of willing participants. Participants had to trust each other and the ACI for JV to work because it required individuals and organizations to potentially expose some hard truths. More importantly, the ACI is constantly fielding requests for JV events throughout the country, and the team is simply too small and the time lines too long for the ACI to scale JV to meet the demand. The ACI cannot stress enough how grateful it is that all the participants engaged with it throughout the JV process, especially with their willingness to trust and be challenged; by making JV development accessible, the team hopes to enable emergency responders at all levels to leverage existing relationships for rapid and effective exercises. By keeping this research objective in mind throughout the process, the ACI hopes to design a tool that is easy to use, allowing cities of any size and budget to plan and execute their own JV events and ACI personnel to focus on conducting research and offering advice when necessary.

4.3. Components

JV comprises three components: the Planning Team, the TTX, and the live-fire exercise (LFX). The latter two are cyber simulations and dependent upon available resources (e.g., employee availability) and capabilities (e.g., access to IT and OT virtual range environments). Component 1, the Planning Team, is the most critical. Component 1 comprises representatives from sector-specific critical infrastructure organizations. The three-component structure gives participants the opportunity to conduct collective cybersecurity training, enhance cross-sector information sharing practices, coordinate technical-level threat information sharing, and communicate effects and risks to management. The LFX, which was canceled because of issues arising from the COVID-19 pandemic, would have exposed participants to threat tactics, tools, and shared techniques.

- **Component 1:** The Planning Team comprises representatives from sector-specific critical infrastructure organizations. Team members, also known as "trusted agents," are key to successful development and execution.
- **Component 2**: The TTX is a simulated and facilitated discussion based on a scenario that takes participants through the process of dealing with a physical disaster blended with malicious cyber activities. Note: This component will be described in greater detail in section 4.7, "Scenario," and Appendix D, "Law/Policy Tabletop Exercise (TTX)."
- **Component 3**: The LFX is a JV exercise component that uses an on-range, simulated, virtual environment. The LFX follows a scenario that correlates with the TTX scenario. It exposes participants to threat tactics, tools, and shared techniques and tests cyber equipment and response capabilities in real time. Note: Due to circumstances beyond the control of anyone planning the event, the LFX was not included in this iteration of JV. It is included in this report because it remains a critical component for the future.

The Planning Committee is the most critical component to the successful planning and execution of a JV event. The JV 3.0 Planning Committee included governmental representatives from Charleston and Savannah, sector-specific critical infrastructure organizations, and the ACI and its partners. The members of the committee took part in one or more working groups, or Operational Planning Teams (OPTs), that directly supported key aspects of JV 3.0. The following are the names and purposes of the OPTs:

- **Lead and Resource Support**: Plan, resource, and coordinate the OPTs to support both the OPTs' purposes and the event's overall objectives.
- **Scenario Design and Execution**: Design and execute an objective-focused event with a realistic and integrated scenario with injects focused on participant-nominated objectives.
- **Data Collection and Analysis:** Identify, understand, collect, assess, and synthesize impactful qualitative and quantitative data that both supports bottom-up resiliency and ensures Army force projection capabilities.
- **Cyber Range Development**: Provide a combination virtual/physical space in which JV event participants can conduct a cyber game scenario using realistic representations of municipality infrastructure.
- **Law and Policy TTX**: Baseline understanding and address underlying concerns about authorities, reporting, and assistance.

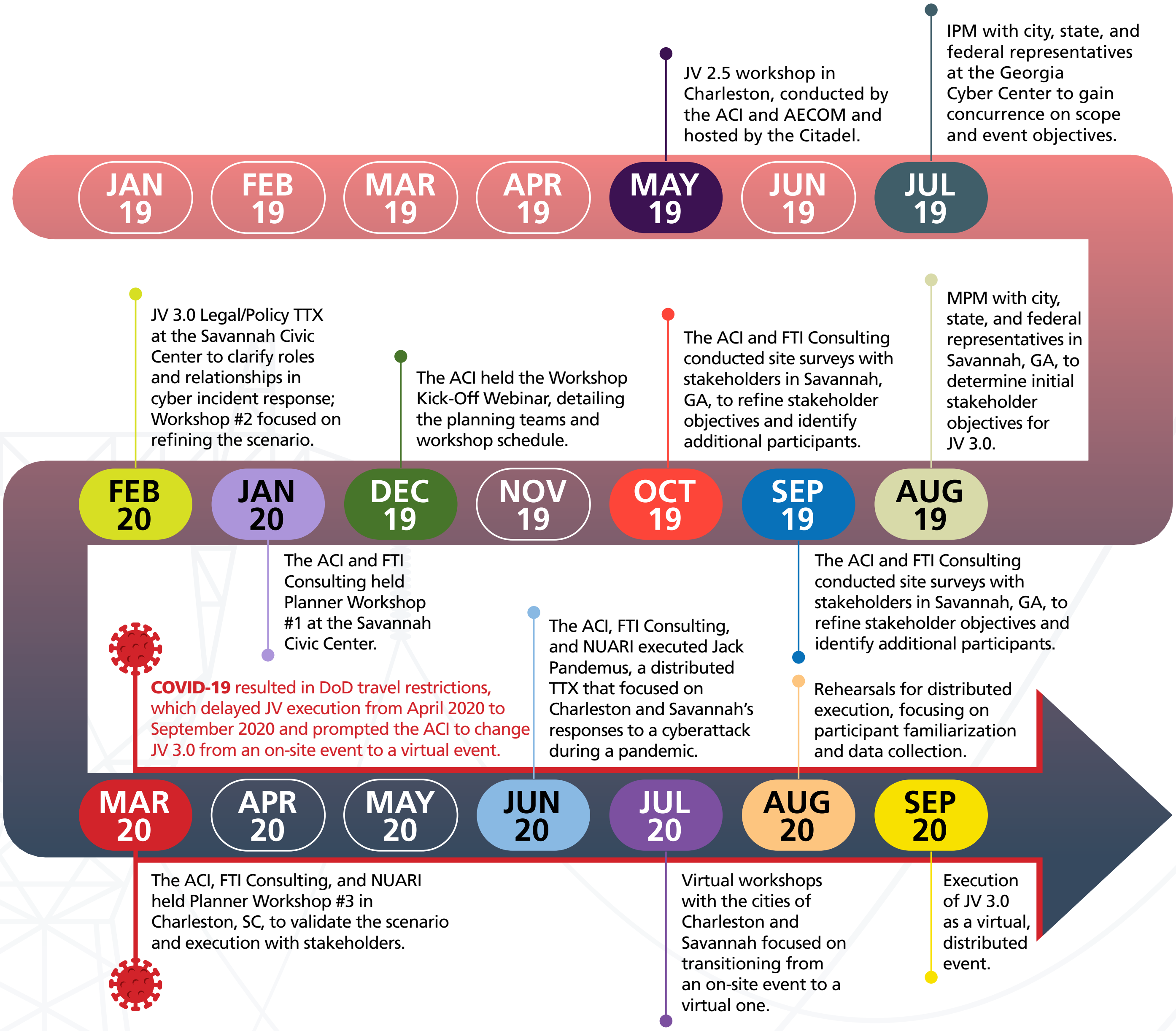
- **Strategic Communications**: Effectively communicate the meaningful stories and messages of JV to key audiences.
- **Distinguished Visitor (DV) Day**: Create an opportunity for Senior Leaders and Executives to experience JV. Note: Due to the COVID-19 pandemic, this OPT shifted to an Executive Out-Brief to provide senior leaders and executives initial feedback on JV 3.0.

Planning for JV 3.0 included multiple planning and rehearsal workshops. The early workshops were designed to start with relationship building and solicit objectives from prospective partners and participants. Later workshops solidified the scenario, confirmed participant rosters, validated that participant objectives and JV research objectives were being addressed, and gave participants multiple opportunities to practice with the technologies that were going to be used to administer the JV events.

4.4. Planning Time Line

The ACI and its partners held a series of planning meetings and workshops that facilitated establishing the membership of the Planning Committee, understanding stakeholder objectives for the exercise, and developing a scenario that would meet stakeholder and event objectives (see Figure 2, "JV 3.0 Planning Time Line"). Prior to March 2020, the Planning Committee met in person for most meetings and workshops. These on-site events allowed the members of the committee to develop strong relationships and trust that eased the transition to virtual events after pandemic-related restrictions took hold.

When the Planning Committee shifted to a virtual execution, they recognized two key challenges: maintaining stakeholder engagement and increasing participant comfort with the required technology. The ACI, NUARI, and FTI Consulting sought to address these challenges by providing stakeholders and participants an opportunity to participate in three separate virtual TTXs. The first, Jack Pandemus, was a 3-hour event that served as a test for virtual execution using both NUARI's DECIDE® and Microsoft Teams. Following Jack Pandemus, the ACI and its partners held two additional 4-hour events using DECIDE® and Microsoft Teams. These rehearsal events allowed the Planning Committee to refine its execution plan and provided participants additional opportunities to gain experience with the event and the various supporting platforms.



JV 2.5 workshop in Charleston, conducted by the ACI and AECOM and hosted by the Citadel.

IPM with city, state, and federal representatives at the Georgia Cyber Center to gain concurrence on scope and event objectives.

MPM with city, state, and federal representatives in Savannah, GA, to determine initial stakeholder objectives for JV 3.0.

The ACI and FTI Consulting conducted site surveys with stakeholders in Savannah, GA, to refine stakeholder objectives and identify additional participants.

The ACI and FTI Consulting conducted site surveys with stakeholders in Savannah, GA, to refine stakeholder objectives and identify additional participants.

The ACI held the Workshop Kick-Off Webinar, detailing the planning teams and workshop schedule.

The ACI and FTI Consulting held Planner Workshop #1 at the Savannah Civic Center.

JV 3.0 Legal/Policy TTX at the Savannah Civic Center to clarify roles and relationships in cyber incident response; Workshop #2 focused on refining the scenario.

COVID-19 resulted in DoD travel restrictions, which delayed JV execution from April 2020 to September 2020 and prompted the ACI to change JV 3.0 from an on-site event to a virtual event.

The ACI, FTI Consulting, and NUARI held Planner Workshop #3 in Charleston, SC, to validate the scenario and execution with stakeholders.

The ACI, FTI Consulting, and NUARI executed Jack Pandemus, a distributed TTX that focused on Charleston and Savannah's responses to a cyberattack during a pandemic.

Virtual workshops with the cities of Charleston and Savannah focused on transitioning from an on-site event to a virtual one.

Rehearsals for distributed execution, focusing on participant familiarization and data collection.

Execution of JV 3.0 as a virtual, distributed event.

Figure 2: JV 3.0 Planning Time Line

4.5. Partners

The ACI works with partners that have mutual interests and that aim to resolve similar issues. Preventing future cyber-related crises can become a reality through establishing public-private, academic, and industry relationships with relevant experts. Furthermore, JV 3.0 and Jack Pandemus (see section 5.1) would not have been possible without these partners.

All partner contributions were truly invaluable and necessary for conducting JV 3.0. Without these partners, JV 3.0 would not have been a success. Full details of each partner's contributions are included in Appendix B, "Partners." The following is a summary of each organization's contributions to JV.

4.5.1. City of Charleston

The City of Charleston, SC, participated in both the planning and execution of JV 3.0. Beginning with the JV 2.5 workshop in May 2019, city staff learned about the history and goals of the JV program. Staff also gained a better understanding of why the ACI and its partners were interested in studying the current security posture of municipal governments and an appreciation of their working relationships with state and federal agencies with respect to the identification of, management of, and response to cyber events. Charleston assisted in identifying potential participants in the region from both the public and private sectors who would likely be impacted by a significant event in the area. In the planning meetings, city staff provided information about the unique geography of the region and interactions among various local agencies, with the goal of providing background information to allow for the creation of an exercise scenario that was germane to the local participants. Representatives from the city's Information Technology, Traffic and Transportation, Police, and Fire departments, among others, actively participated in the TTX.

4.5.2. Town of Mount Pleasant

The Town of Mount Pleasant, which is located across the Cooper River from Charleston, provided integral support from the JV 2.5 Cyber Workshop Series through the planning and implementation of JV 3.0. In addition, Mount Pleasant provided leadership in decision support for the unique challenges arising from the impacts of COVID-19. Mount Pleasant's emergency manager served as a regional point of contact for the exercise and ensured participation from stakeholders and partners. Early on, Mount Pleasant hosted events with critical infrastructure representatives to introduce the ACI and collaborate on SC cybersecurity concepts and issues. These events allowed for the sharing of unique regional insights and provided groundwork for the initial planning phases of JV 3.0. Furthermore, Mount Pleasant's Information Technology department worked in concert with the City of Charleston to coordinate information sharing among players and stakeholders. This work strengthened Mount Pleasant and Charleston's partnership and overall cyber readiness and posture.

4.5.3. City of Savannah

The City of Savannah, GA, was involved early in the planning process. Led by the City of Savannah emergency management director, the IT, emergency preparedness, fire, and water resources departments became significantly involved in the planning. Savannah's emergency manager and IT department served as the city's points of contact for the exercise, introducing ACI to critical stakeholders in the area. In addition to supporting and attending the ACI meetings, Savannah held its own internal meetings to discuss and determine participation. The city also finalized its Cyber Incident Annex as part of its preparation. Savannah had 18 personnel from multiple agencies participate in the Rehearsal of Concept (ROC) Drills and exercise. The local police department participated in the ROC Drills, but it could not make the final exercise because its participation was preempted by a real-world incident.

4.5.4. FTI Consulting

Because JV research emphasizes the need for public-private partnership and a whole-of-community approach, the ACI recognizes the need for private expertise to make JV events valuable. To that end, the ACI was proud to partner with FTI Consulting for JV 3.0. FTI Consulting is a global business advisory firm dedicated to helping organizations manage change; mitigate risk; and resolve financial, legal, operational, political and regulatory, and reputational and transactional disputes. More than a dozen FTI Consulting team members, including senior executives and sector subject matter experts, participated in JV 3.0. As recognized leaders in organizational cybersecurity from both technical and policy perspectives, FTI Consulting provided invaluable planning, leadership, and technical expertise to the development, execution, and publicity of JV 3.0 throughout the process, especially in the areas of scenario development and executive communication.

4.5.5. NUARI/DECIDE®

NUARI partnered with the ACI for JV 3.0. NUARI is a 501(c)(3) nonprofit organization that serves the national public interest through the interdisciplinary study of critical national security issues. NUARI is partially funded by DHS and the DoD and federally chartered under the sponsorship of Senator Patrick Leahy. NUARI provides cyber exercises, secure network monitoring, custom consulting, research, and education through many avenues, including its DECIDE® platform exercises. During planning, the DECIDE® platform was intended to serve as the primary means of distributing full information about scenario events and capturing participant responses, with in-person facilitation and conversation serving as an alternate means. When COVID-19 effectively prevented all in-person events, the DECIDE® platform became the sole platform for conducting the virtual TTX. JV 3.0 would not have happened without DECIDE®.

4.5.6. AT&T/FirstNet

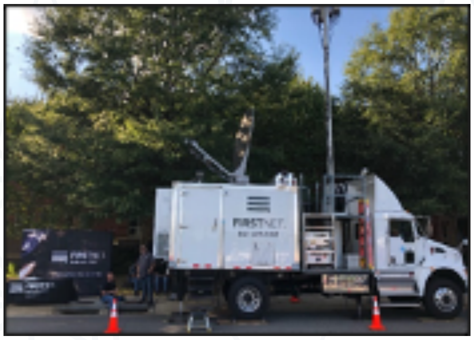


Figure 3: This AT&T SATCOLT is one of the tools that would have served as contingency communications infrastructure for JV 3.0 pre-COVID-19

FirstNet is the Nationwide communications platform dedicated to America's first responders and public safety community, built with AT&T in a public-private partnership with the First Responder Network Authority. Prior to the pandemic, AT&T worked with the ACI to provide a full suite of advanced tools that would serve as the contingency communications infrastructure for the JV 3.0 exercise. These tools included two satellite on light trucks (SATCOLTs), 60 FirstNet-enabled devices, projection monitors, and a team to support the ongoing communications among the participants from local, state, and federal entities. AT&T also planned to provide the ACI with a video team to capture each exercise incident as it unfolded to create a documentary of the events in Charleston and Savannah. When the JV 3.0 event was moved to a virtual format due to COVID-19, AT&T provided a team of subject matter experts in emergency communications, who participated in both the online event and numerous planning sessions to educate the participants and provide guidance on crisis communications, restorative procedures, and FirstNet. AT&T's participation in the planning, execution, and data analysis contributed greatly to the quality of the event and this report.

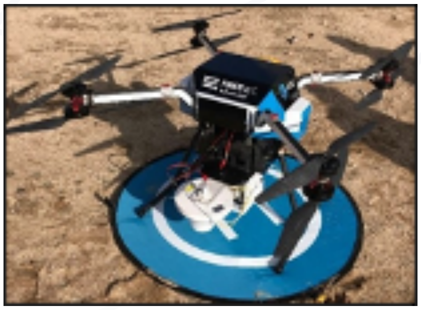


Figure 4: This AT&T cell on wings, also called a "flying COW," would have been one of the FirstNet-enabled devices provided during the JV 3.0 LFX.

4.5.7. Intrepid Networks

Intrepid Networks provides Intrepid Response, a FirstNet-certified and affordable web and mobile situational awareness software platform for day-to-day and emergency operations. Originally, the ACI partnered with Intrepid Networks to furnish licenses to use Intrepid Response on FirstNet phones that would have been provided by AT&T to participants. This would have provided an additional common operating picture platform to achieve realism during the TTX. Intrepid Networks continued to partner with the ACI after the in-person events were canceled and generated exercise common operating picture maps that coincided with scenario events, giving participants the ability to engage with the scenario based on specific urban geography; this achieved an effect like that of Intrepid Response. Intrepid Networks' contribution significantly improved the quality of engagement and the realism of the scenario.

4.5.8. The Citadel

The Citadel hosted a JV 2.5 workshop in Charleston on May 21, 2019. The college worked with the ACI to organize the workshop. In addition, faculty from The Citadel supported the planning efforts, attending the JV 3.0 Initial Planning Meeting in Augusta, GA, on July 9–10, 2019; numerous planning workshops; and the ROC Drill for Charleston on September 8, 2020. Faculty and students from The Citadel participated in the exercise itself, serving as both participants and data collectors.

4.5.9. Savannah Technical College

The ACI and Savannah Technical College (STC) began working together in January 2020. STC provided academic advisory support and facilitated face-to-face meetings prior to COVID-19. Also prior to COVID-19, the ACI and key partners completed a site visit and chose STC as the on-site location for the Savannah JV 3.0 exercise. More than 15 students registered to help as data collectors for the Savannah iteration. This both facilitated the success of JV 3.0 data collection and allowed students to gain valuable knowledge and insight into an aspect of cyber readiness needs and methods that could not be taught solely in the classroom. In addition, STC served as a member of the Distinguished Visitor Day and Scenario Design and Execution OPTs. In the future, STC will continue to collaborate with the ACI by incorporating the JV experience into future training exercises in the coastal GA region.

4.6. Participants

Sector	Charleston	Savannah
Transportation	SC Port Authority	GA Port Authority
	Southeastern Freight Lines (trucking company)	
	US Coast Guard	
	841st Transportation BN (597th TRANS BDE, SDDC)	
	Charleston Traffic & Transportation	Savannah Airport Commission
Energy	Dominion Energy	Georgia Power / Southern Co.
	Dominion Energy Gas	BP
Emergency Management	SLED	GEMA
	City of Charleston EM	Chatham County EM
	City of Charleston FD	Chatham County PD / 911
	Town of Mount Pleasant EM	City of Savannah EM
		City of Savannah PD & FD
Communications	AT&T Local Solutions	
	AT&T Public Sector Solutions (FirstNet)	
Information Technology	City of Charleston IT	Chatham County ICS
	Town of Mount Pleasant IT	City of Savannah IT
	DHS CISA Region IV	
Government Facilities	City of Charleston	City of Savannah
	Charleston County School District	Chatham County School District
Water / Wastewater		City of Savannah Water

Additional Participants:

GA NG, SC NG, FEMA Region IV, 3ID, USAG Fort Stewart, DOE, ARCYBER, ARNORTH, Blank Slate Solution, DCO Region IV, FBI, City of Hinesville, Chubb Insurance, M.C. Dean, Nevada Cyber Solutions, SoCal Gas, Atlas Cybersecurity

White Cell and Research Support:

- Blank Slate Solution
- The Citadel
- DISA
- FTI Consulting
- Idaho National Laboratory
- Intrepid Networks
- JHU APL
- NUARI
- Savannah Technical College
- SLED
- 3ID
- University of Illinois CIRI
- University of South Carolina
- U.S. Army War College

Table 1: JV 3.0 Participants

4.7. Scenario

Information overload is a serious problem with which to contend in both real-life emergency response and fictional exercises. Policies and procedures regarding information sharing are often crafted to streamline distribution of preidentified information types to the most relevant parties. Experienced personnel therefore know and handle much more than is communicated. Because of this filtering of communication, prebuilt relationships are extremely valuable. However, when truly new situations arise for which there are no established policies or practical experience available, information sharing can be slow and inappropriately distributed. Highlighting this difficulty, previous JV events and workshops have revealed cyber incident policies and information sharing agreements that are often incomplete or nonexistent. This was the impetus behind the creation of the JV scenario.

The scenario was the primary method for pursuing the research objectives. Because JV brings together individuals and organizations with diverse and valuable expertise, and no one organization is the single source of expertise and best practices, bringing everyone together to play a fictional game is often the best way to tease out relevant knowledge from the best people in place to handle emergency situations. These conditions create a collaborative learning environment in which we can pursue our research objectives.

4.7.1. Design Requirements

The scenario design needed to accomplish many goals simultaneously:

- Support both the event research objectives and the participant objectives.
- Maintain realism. All injects included in the scenario, especially cyber incidents, were either sourced from real events or forecasted in scholarly works. This ensured relevance and minimized the threat of participants balking at the scenario and refusing to participate.
- Achieve ambiguity regarding severity and the cause of the damage, whether it was equipment failure resulting from normal physical degradation or a cyber intrusion. In other words, the cyber incidents in the scenario needed to avoid being obviously cyber-related.
- Achieve ambiguity regarding the level of sophistication of an actor. In other words, the cyber incidents needed to not be so sophisticated that only a nation-state actor would be capable of performing the attack.
- Keep incidents below a threshold of armed conflict.
- Focus cyber intrusions on local municipality and private entities.

Additionally, the designed scenario introduced a certain level of stress prior to the cyber incidents. Because an adversary would most likely time its intrusions and disruptions to have a maximum impact, it was important for local resources to already be in place to deal with other, noncyber issues. For this reason, protests, traffic issues, and natural weather considerations were included in the scenario to ensure participating emergency responders were already expending planning, personnel, and materiel resources before the additional events occurred.

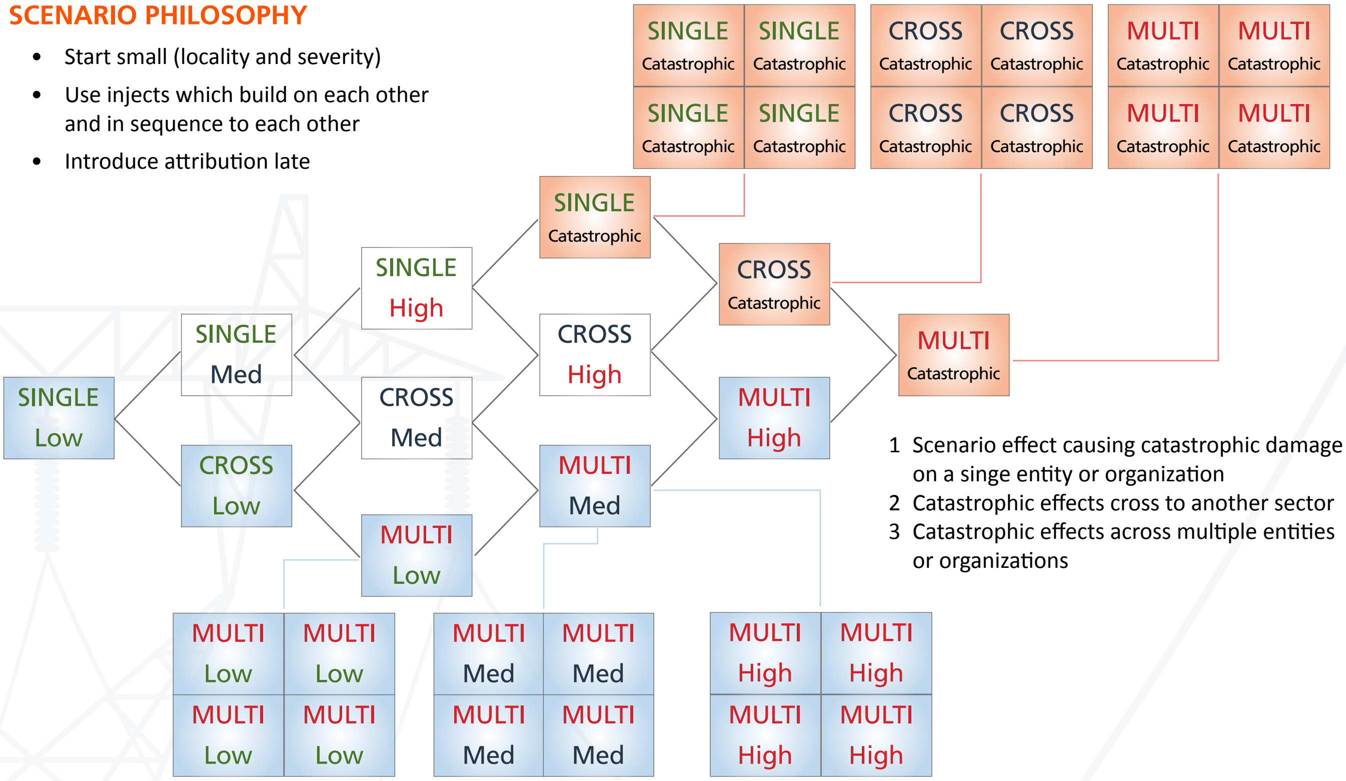
4.7.2. Design Concepts

In designing the scenario, the Planning Team's strategy was to use injects that progressively built upon one another, avoid introducing attribution, and keep incident causes ambiguous for as long as possible. This "death by a thousand cuts" approach allowed the ACI and its partners the opportunity to explore thresholds at which organizations would identify a cyber incident and request support. Keeping the cause of the incident ambiguous facilitated debate among participants, encouraged them to share their decision-making processes with other participants, and increased the realism of the exercise.

The scenario was designed to be played over a series of turns and to weave together multiple independent threads—a set of sector-specific injects that build on themselves—to form a cohesive story. Each thread was built such that its specific injects would grow progressively more dangerous, either by spreading to new areas, organizations, or systems or by causing increased amounts of damage to affected entities. During the planning workshops leading up to JV 3.0, it was evident that many participating organizations, particularly in the municipalities, lacked the resources to adequately defend against a sophisticated adversary. Therefore, the Planning Team designed the scenario from a perspective of assumed compromise. Many of the scenario parameters, such as when malware exploitation would migrate from sector to sector, were deliberately kept opaque to the players. This approach forced participants to respond to incidents rather than attempt to defend against them. See figure 5 for a graphical display of the expected progression.

SCENARIO PHILOSOPHY

- Start small (locality and severity)
- Use injects which build on each other and in sequence to each other
- Introduce attribution late



1 Scenario effect causing catastrophic damage on a singe entity or organization
2 Catastrophic effects cross to another sector
3 Catastrophic effects across multiple entities or organizations

ENTITY	DAMAGE
Single: One organization	**Low:** Internally inconvenient or not noticeable, no noticeable external effect
Cross: Two organizations	**Medium:** Internally disruptive, externally inconvenient
Multi: Three or more	**High:** Internally destructive, externally disruptive
	Catastrophic: Serious economic damage and/or some loss of life, serious disruption or damage to dependent organizations

Figure 5: JV 3.0 Scenario Development Framework

Following this design philosophy allowed several important benefits:

- Creative freedom could be given to multiple independent scenario writers, each with his or her own expertise (for example, the energy sector), without hindering other writers’ efforts.
- Starting small with each thread ensured no one thread would dominate the scenario because of how it was written. Thus, if the scenario incidents caused the conversation about one specific thread to become dominant during the JV 3.0 event, this would be useful information for data collectors.
- There was more going on in the scenario than participants could see. Because DECIDE® was able to distribute injects to participants based on their roles and responsibilities, any thread that was not discussed due to lack of participation would simply not be part of the conversation. This ensured

that all players were able to participate based on their personal and expected expertise, without relying on players to inexpertly speculate on the activities of organizations not able to participate.

- The slow progression of each thread meant the overall scenario difficulty would increase incrementally from turn to turn, thereby allowing a more organic discussion of the thresholds for responses, declarations, and requests.
- This algorithmic approach makes it possible to combine any number of independent threads to create unique scenarios quickly, depending on focus and need. This benefit supports the automation project discussed later in this report.

4.7.3. Validation

During the leading workshops that occurred throughout the planning and development process, the Planning Team tested the scenario. Through repeat rehearsal and refinement, the Planning Team not only validated each individual thread, but also provided the basis for understanding expected responses to the scenario elements. This allowed the scenario development team to build a realistic and challenging scenario that ultimately maintained engagement during the JV events and supported the data collection and analysis to successfully address the research and participant objectives.

4.8. Data Collection and Analysis Plan

JV 3.0 incorporated a stakeholder-driven, multipronged data collection approach. The primary goal was to collect and analyze meaningful data to help build critical infrastructure and emergency response capacity and resiliency at a municipal level and to inform Army tactical, operational, and strategic calculations regarding potential impacts on force projection capabilities. Accordingly, the data collection and analysis plan was designed to identify critical information that could help answer the overarching JV 3.0 research objectives previously identified. The following sections go into greater detail about these objectives.

4.8.1. Developing the Data Collection and Analysis Plan

Creating an effective data collection and analysis plan required the identification of key stakeholders and information requirements for each research objective referenced above. Each of the three JV 3.0 planning workshops included sessions for developing and refining data collection and analysis procedures to ensure stakeholder critical information requirements were identified during the preliminary planning and design phases of the event. Once the relevant issues were identified for key city, county, state, federal, military, and private sector stakeholders, an information synchronization matrix was constructed to visualize appropriate indicators and information requirements to support the achievement of the research objectives. Additionally, key supporting stakeholder requirements were outlined to facilitate better understanding of all potential areas for data collection and analysis efforts during JV 3.0. This stakeholder-informed methodology resulted in the identification of: (1) specific information requirements to support primary JV 3.0 research objectives; (2) a coalition of willing stakeholders to help support data collection and analysis; and (3) potential gaps in data collection and analysis.

The critical steps in plan development included:

- *Identifying* strategic research objectives;
- *Nesting* stakeholder objectives within this strategic research framework;
- *Determining* data objectives and *synchronizing* intersecting areas of interest;
- *Cataloging* all available resources in support of data collection and analysis to identify redundancies, interdependencies, and potential gaps;
- *Verifying* essential elements of information, key indicators, and methods of collection on available platforms; and
- *Designing t*he most advantageous data categorization scheme to facilitate post-event analysis and support the generation of the final report.

4.8.2. Workshops and Stakeholders

Creating a coalition of willing partner organizations was a key facet of the JV 3.0 data collection and analysis. These partner organizations were integral contributors to survey question design, organizational data collector support, data postprocessing, data visualization, and the production of key areas of this final report. To further synchronize and enhance this support given the change to a distributed execution, the ACI hosted three data collection and analysis workshops prior to the JV 3.0 exercises with participation from state, military, academic, and private sector partners. The key takeaways of these workshops are detailed below.

Workshop #1: June 2020

- Reaffirmed and further solidified data collection and analysis partnerships for JV 3.0 as the team worked toward event execution;
- Generated additional participation and support for data collection and analysis during the Jack Pandemus mini-exercise (described later in this report);
- Created new partnerships both for the ACI and within the larger data collection and analysis team;
- Ensured a clear understanding of and consensus on data collection and analysis efforts before event execution; and
- Established redundancy in collection platforms, methods, and constructs to ensure a robust dataset for holistic post-event analysis.

Workshop #2: July 2020

- Reaffirmed and further solidified data collection and analysis partnerships for JV 3.0 as the team worked toward event execution;
- Identified lessons learned and areas for refinement following the execution of the Jack Pandemus exercise; and
- Created a common operating picture of holistic and robust support for JV 3.0 data collection and analysis.

Workshop #3: August 2020

- Revalidated commitments and updates for partners and participants;
- Finalized data collection approaches, platforms, and tools to be used during the JV 3.0 event;
- Presented and discussed survey question development, methodology, refinements, comments, and recommendations prior to event execution;
- Refined and recommended final data collector guidance; and
- Established an additional working group to support partnerships and new ways to facilitate additional collaboration going forward.

Numerous stakeholder organizations participated in these workshops and volunteered to support data collection and analysis planning, execution, and postevent efforts. Participating organizations included:

- U.S. Army War College
- University of Illinois at Urbana-Champaign (UIUC) Critical Infrastructure Resilience Institute (CIRI)
- NUARI
- Idaho National Laboratory (INL)
- Johns Hopkins University Applied Physics Laboratory
- 3rd Infantry Division (3ID) Headquarters
- Military Surface Deployment and Distribution Command (SDDC)
- 597th Transportation Brigade
- 841st Transportation Battalion
- Center for Army Analysis
- Intrepid Networks
- SC Law Enforcement Division (SLED)
- FTI Consulting
- The George Washington University
- Provatek
- Blank Slate Solution

4.8.3. Continued Refinement and Validation

Validation and continuous refinement of the data collection and analysis plan occurred across multiple smaller events leading up to the JV 3.0 events. Validation and proof of concept events included:

- *Jack Pandemus*—Pandemic-based cyber incident scenario exercise distributed through the DECIDE® platform and Microsoft Teams.
  - » Allowed for initial validation of survey question structure and delivery and DECIDE® platform data collection functionalities.
- *ROC Drill #1*—Initial scenario delivered to participants in a controlled environment in preparation for event execution.
  - » Revalidated survey question structure and delivery and DECIDE® platform and Microsoft Teams meeting process and data collection functionalities.

- *ROC Drill #2*—Initial scenario delivered to participants in a controlled environment in preparation for event execution.
  - » Finalized survey question structure and delivery and DECIDE® platform and Microsoft Teams meeting process and data collection functionalities.

4.8.4. Data Sources

To facilitate robust data collection, multiple platforms and functionalities were built into the overarching data collection approach, as described in table 2.

Data Type	Collection Platform	Functionality	Description
Raw	Microsoft Teams	Audible discussions	For each segment, participants discussed responses to the scenario information, both at the virtual table for their respective sectors and the main table with all participants.
Raw	Microsoft Teams	Text chat panel	Participants sometimes typed discussion points in the Teams chat. Data collectors inserted those comments into the DECIDE® chat log (row 4).
Raw	DECIDE®	Emails or chats initiated by participants	To request information and coordinate responses to the injects, participants could communicate with each other in writing in DECIDE® via a global chat channel, by creating a new chat group, or via email. Participants rarely used this functionality.
Structured	DECIDE®	Table and White Cell chat channels	For each virtual table, a chat channel was created in DECIDE® for exercise controllers and data collectors to log data gathered from participant discussions at individual and main tables. These data entries were preceded by a code/tag from the data coding scheme.
Structured	DECIDE®	Online surveys (preexercise, between turns, and postexercise)	Participant surveys were delivered preexercise, between turns, and postexercise. The DECIDE® survey area contained a text box (observation pane) that data collectors could use to log observations, but this box did not timestamp the entries, and collectors were advised to use chat (row 4) instead.

Table 2: JV 3.0 Data Sources

4.8.5. Data Coding Schema

A data classification coding scheme was developed for categorizing the exercise observations to assist in postprocessing efforts following execution. Data type tags, classification descriptions, and examples were outlined for data collectors prior to the event and included in the *Jack Voltaic 3.0 Data Collector Guide* distributed to all volunteers. Some of the data tags used in the JV 3.0 exercises are listed in table 3.

Data Tag	Description	Data Tag	Description
Meta	Exercise design, platform, or logistics	Strength	Demonstrated capability, knowledge, or available resources
Turn	Signaled a changeover between turns	Comm	Communication, information sharing, or relationship formation
Msg	Messages between data collectors and exercise controllers	Cikrdep	Identified critical infrastructure dependency or interdependency
Focus	Table-focused areas of discussion	Dodaid	DoD incident response support provided or available
Plan	Information on plans in place and thresholds/criteria for initiating plans of action	Forcep	Information regarding or impacts on force projection capabilities
Action	Participant decisions/actions on how to respond to the current situation	Abs	Relevant stakeholders who were not present
Gap	Missing information, resources, or context necessary for decisions or response actions	Keythread	Discussion thread from individual tables to be discussed at the main table

Table 3: JV 3.0 Data Tags

4.8.6. Data Collector Guidance Development and Training

Data collection and analysis planning culminated in the *Jack Voltaic 3.0 Data Collector Guide*, which was distributed to volunteer data collectors. The guide includes primary data collector responsibilities; classification codes for DECIDE®; and a common concept for capturing data, platforms, and mechanisms.

Additionally, the Data Collection OPT conducted training sessions for volunteer data collectors and exercise controllers to ensure proficiency in platform features and data coding and familiarity with virtual table assignments. The second training session, which included an overview of the hypothetical scenario, allowed data collectors to practice logging data into DECIDE® (row 4 in Table 2, "JV 3.0 Data Sources") using the data codes as they listened to a mock discussion among three "participants" (members of the JV 3.0 organization team).

5. EXECUTION

Most of JV 3.0 planning revolved around an in-person exercise, originally scheduled for April 28–30. When COVID-19 forced the cancellation of the in-person event, planners had to shift to a completely virtual format. The final execution events took place on September 22 for Charleston, SC, and September 24 for Savannah, GA.

This chapter outlines how the JV execution events were administered. It discusses the composition and responsibilities of participants, the White Cell, and data collectors; the ROC Drills; the execution of the main events; and the ACI's utilization of technical platforms to host the virtual exercises. First, however, we discuss the impact of COVID-19 as well as the rapidly developed Jack Pandemus exercise.

5.1. Coronavirus Disease 2019 (COVID-19) / Jack Pandemus

The most important partner-participants in JV are, and always will be, the municipal-level individuals and organizations. In particular, the emergency managers of participating cities have the responsibility and existing relationships to bring together the best coalitions for their respective areas. When it became clear that COVID-19 would not only interrupt JV 3.0, but also dominate real-life local incident planning and response for the foreseeable future, the main research objectives of JV became less urgent for these key partners. As a result, the Planning Team had to decide whether to introduce the pandemic, a topic on everyone's mind, into JV 3.0. Additionally, the cities of Charleston and Savannah face hurricane season each year during the summer and early fall, thus pushing back any possibility of rescheduling a JV event to late September. Such a delay risked a loss of momentum for JV and a loss of engagement with all partners and participants. Fearing that the pandemic would be a confounding variable and make studying cyberattack response more difficult, the Planning Team decided to produce and conduct a virtual event that incorporated the pandemic into the scenario and used the same techniques and platforms as JV. The purposes of the resulting exercise, dubbed "Jack Pandemus," were to:

- Address participant concerns about cyber incident response during the current pandemic crisis;
- Reengage the coalition of partners and participants with a highly relevant exercise and generate fresh momentum toward a rescheduled JV 3.0; and
- Execute a trial run with the technical platforms planned for JV use to familiarize planners, facilitators, and participants with the technologies and their capabilities.

5.1.1. Conduct of Jack Pandemus

The ACI, in partnership with FTI Consulting and NUARI, executed Jack Pandemus twice: once for Charleston on June 23, 2020, and once for Savannah on June 30, 2020. The two-hour virtual TTXs used the DECIDE® platform to play through a hypothetical scenario that included a cyberattack on the local natural gas company and a gas pipeline disruption directly impacting electrical power generation and healthcare delivery.

The Jack Pandemus scenario occurred in the context of an ongoing pandemic response. The scenario included government-ordered shutdowns, nonpharmaceutical interventions, personal protective equipment shortages, and protests. During these challenges, a cyber intrusion at a gas company caused an explosion at a natural gas relay. Already short on personnel and with its resources overtaxed, the local government was forced to request assistance through the county emergency operations center to the state's emergency management division.

5.1.2. Jack Pandemus Summary Findings and Feedback

As with JV, the scenario was designed to emphasize the holistic, multisector nature of incident response. Participants gained a much greater appreciation of both their cross-sector dependencies and the dependencies of other organizations and were often surprised how cyberattacks could have ripple effects. The event highlighted numerous sector interdependencies among hospitals, local schools, local vendors, power companies, state emergency operations, and the defense coordinating element (DCE). As a result, participants realized the importance of establishing relationships prior to a crisis.

Regarding municipal readiness, the scenario highlighted the significant disconnect between the resources available and the resources that were needed. City and county personnel were concerned with how quickly municipal resources were being exhausted and sought any available state and federal resources for cyber incidents. The scenario events' ambiguous cause—cyberattack or equipment malfunction—confused communications between participating organizations. Due to this ambiguity, participants noted the critical need for clearer legal authorities, well-defined response procedures, and priorities for resources allocation prior to a real crisis.

The consensus among participants was that Jack Pandemus achieved its objectives and was a resounding success. Participants appreciated the challenging nature of the scenario and the lessons learned; most wished the scenario could have been longer than 2 hours. The ACI conducted a follow-up webinar on July 19, 2020, to review necessary changes to the JV 3.0 exercise in response to the pandemic. The successful execution of Jack Pandemus allowed participants and administrators to give essential feedback on the virtual, distributed execution which the Planning Team incorporated into the JV 3.0 rehearsals and main event.

5.2. Event Design

JV 3.0 was originally designed to be an in-person 3-day event. Changing to a virtual, single-day event while ensuring maximum value from the interactions between participants proved to be a significant challenge. However, the initial groundwork done by the Planning Team meant that the final event was effective and engaging. At both events, over 95 percent of participants stayed through the entire exercise, and everyone who participated contributed something during the event. This section describes the final design and the decisions and circumstances that determined how JV 3.0 was conducted.

5.2.1. Virtual Execution

There are many reasons to prefer in-person drills and exercises, including the benefits of an LFX, enhanced opportunities for discussion, and increased relationship building in general. However, the success of Jack Pandemus showed an incident response exercise could meet objectives in a virtual, distributed setting, and feedback from Jack Pandemus showed how virtual tables (breakout rooms) could be used to encourage engagement. Technology platforms allowed for the effective dissemination of information, organized and facilitated discussions, participant feedback, and data collection. Although a virtual event necessitates controlled communications—using the "raise your hand" function in Microsoft Teams, for example—the format allows all conversations to effectively be captured by data collectors. Also, having participants distributed throughout various locations in real time simulated a real incident response scenario.

5.2.2. Technology Platforms

During the virtual events for each city, attendees used Microsoft Teams to participate in and move between plenary discussions at the main table and assigned, small-group tables designed to replicate actual interactions within organizations during incident response. Participants needed to log into two separate Microsoft Teams meetings—one for each of these tables. Participants were assigned tables based on their organization or responsibility and were instructed to remain at the assigned tables throughout the exercise. In addition to oral participation via Microsoft Teams, participants could hold side discussions in the Teams chat, and all of this data was analyzed by data collectors.

The DECIDE® platform, described in section B.2.4 of this report, allowed participants to visualize scenario information, send and receive communications, and answer survey questions. Participants saw three panes on the DECIDE® screen: a communication pane highlighted in green, an information pane highlighted in yellow, and an action pane highlighted in orange. Data collectors and event controllers used a DECIDE® chat line to log critical participant discussions and a separate DECIDE® chat channel to log meta observations.

5.2.3. White Cell

The JV 3.0 exercise was administered by an exercise team, or “White Cell” (see Figure 6, “Exercise Team [White Cell]”). White Cell personnel were assigned to several different roles:

- The **exercise lead** was responsible for the overall conduct of the event, including planning and platforms, dealing with changes, and providing guidance to the White Cell members. The exercise lead also engaged with the participant organizations’ points of contact.
- The **facilitator lead** guided event discussions at the main table to meet drill objectives and, as such, needed to thoroughly understand the event scenarios and participant organization responsibilities. This role required striking a delicate balance between guiding the discussions and allowing for freedom of thought and action. Specific responsibilities included coordinating the overall event with the exercise lead; managing the information injects, including any necessary changes to them; monitoring participant responses and stress levels; encouraging interorganizational engagement; identifying gaps in policy or process; assessing cities’ incident response preparedness; and overseeing the event controllers and DECIDE® platform personnel.
- The **event controllers** support a particular table of players, serving as both the communication link for the players to the White Cell and facilitator for the players at their discussion tables. The event controllers acted as communication bridges between the individual tables and the White Cell, using the Microsoft Teams White Cell chat line to summarize decisions made by the discussion table and points of discussion that would be of interest to the larger group. The event controller also used the DECIDE® White Cell chat channel to record metaobservations for event improvement. Other responsibilities included maintaining the event schedule, supporting participant use of DECIDE® and Microsoft Teams, and providing a summary of the events of the turn if necessary.
- The **data collectors**[21] captured critical observations, primarily using the DECIDE® platform, but also Microsoft Teams for redundancy, as the scenario unfolded. Data collectors were assigned to specific sectors or groups of interest; they also filled gaps in coverage when necessary. Following the Jack Voltaic 3.0 Data Collector Guide, data collectors familiarized themselves with the

[21] Data collector roles and data collection and analysis in general are described in section 4.8, “Data Collection and Analysis Plan.”

DECIDE® platform to document details of participant reactions and interactions. They captured probing questions posed by participants and communication or relationship gaps and identified interdependencies among people or organizations. Data collectors focused on critical insights during incident response, including:

- Information, communication, and operational gaps discovered;
- Newly identified interdependencies between participants;
- Gaps and interdependencies that affected or concerned an organization;
- Newly formed relationships, groups, and structures created during each scenario turn;
- Actions assigned sectors took to mitigate the impacts of the cyber incident and scenario injects;
- Internal and external information-sharing mechanisms of assigned sectors;
- Interactions, collaborations, and friction points between the public and private sectors as the scenario unfolded; and
- New and/or existing thresholds for requesting additional support during response efforts.

- **DECIDE® controllers** managed the DECIDE® experience of each event, including planning; building; deploying; operating; maintaining; and adjusting, if necessary, a functional environment to support the event. They troubleshot and addressed any technical issues with the platform and assisted event controllers during the event.

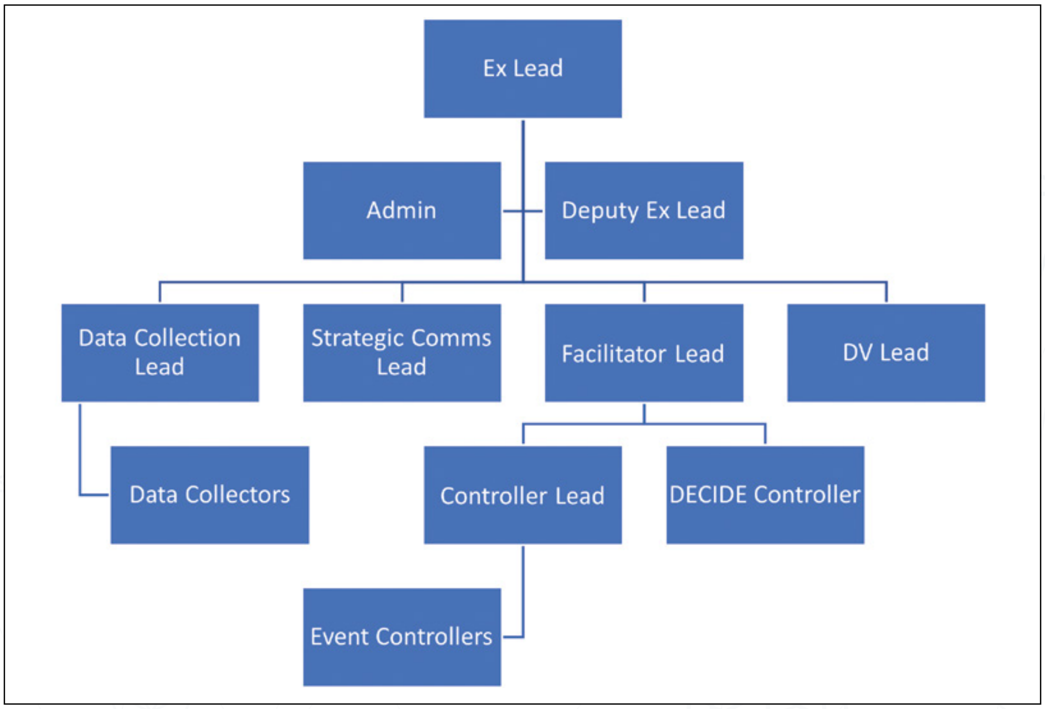


Figure 6: Exercise Team (White Cell)

5.2.4. Event Format

Each single-day event began at 8:00 a.m. and concluded at 4 p.m. Participants played the scenario over a series of turns, and each turn included three phases (see Figure 7, "Turn Phases"):

- Phase 1—Assess (approximately 10 minutes): The Assess phase was focused on the individual participant and his or her interaction with DECIDE®. During this phase, participants received their sector-specific injects and had time to digest the incoming information. Participants were encouraged to use DECIDE® communication features to contact participants at other tables to facilitate their discussions.
- Phase 2—Discuss (approximately 15 minutes): The Discuss phase allowed participants to discuss the current situation with the other participants at their discussion tables. For JV 3.0, there were eight discussion tables:
  - City table
  - County table
  - State table
  - Health and medical table
  - Port and port operations table
  - Energy table
  - Federal table
  - Private sector table

During this phase, the objective of the discussion was to determine:

- What injects were most relevant to the organizations/roles at this table?
- What existing plans applied to these issues? Were there issues that were not covered by a plan?
- What decisions would you make in responding to the inject?
- What actions would you take in responding to the inject? If you would not take an action, why not?

Players could request information from an agency or sector not participating in the event by reaching out through the DECIDE® platform or notifying the discussion table's event controller. Upon conclusion of this phase, participants transitioned to the next phase.

- Phase 3—Integrate (approximately 45 minutes): The final phase, Integrate, was community-focused and leveraged Microsoft Teams for a facilitated discussion on how the various organizations responded to the events of the turn. This phase required all participants to interact with the facilitator lead at the main table, which included all participants and the White Cell. During this phase, the facilitator lead had participants share their findings from the previous two phases with the community through directed and open-ended questions. At the end of this phase, participants completed survey questions.

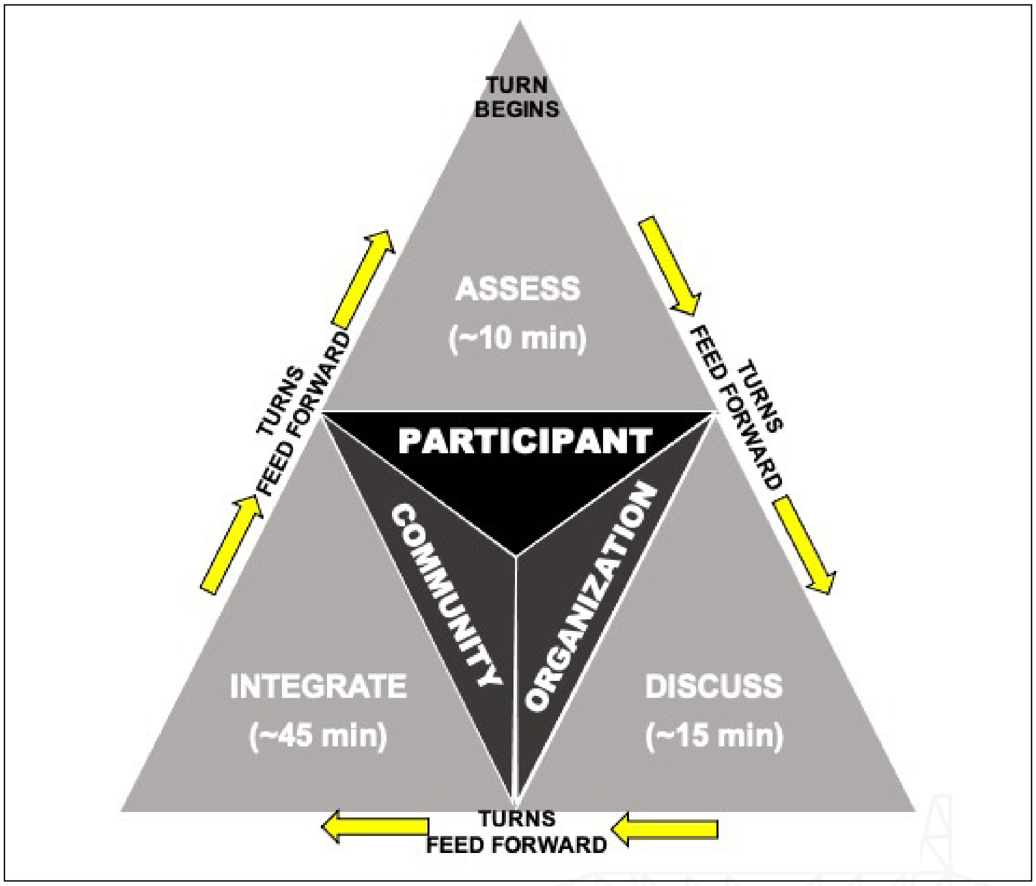


Figure 7: Turn Phases

During each phase, data collectors used the DECIDE® platform to record observations based on their assigned areas.

5.2.5. Rehearsal of Concept Drills

Four ROC Drills were held virtually: two for Charleston on August 18, 2020, and September 8, 2020, and two for Savannah on August 20, 2020, and September 10, 2020. The goals of the ROC Drills were to further familiarize participants with the tools and to refine processes planned for use in the JV 3.0 exercises. Because JV 3.0 was originally intended to be a 3-day event, the scenario developed for JV 3.0 was too long for a single day. Rather than lose any value for unplayed turns, the drills provided an opportunity to introduce the scenario and the first four turns of the scenario. Lastly, the drills allowed the data collection team to practice the procedures in the *Jack Voltaic 3.0 Data Collector Guide* prior to JV 3.0.

The ROC Drills followed the same basic structure with respect to technical platform, player and White Cell roles and responsibilities, and event format as the main event, except that each drill was a 4-hour event. The first drill for each city included turns 1–3, and the second drill included turns 3–4. See table 4 for the schedule of the second ROC Drill. This effectively familiarized players and White Cell personnel with the scenario and helped solidify the format of the main event. In every drill—and, to a lesser extent, the main event—there were log-in and other technical issues, so overlapping the last turn of the rehearsal with the first turn of the main event mitigated the effect of some participants struggling to join on time.

Time (EST)	Event	Location
8:30 – 8:50 AM	Welcome and Scene Setter	Main table
8:50 – 9:00 AM	Preevent Survey Questions	DECIDE®
9:00 – 9:25 AM	Turn 3 (Assess / Discuss)	Discussion table
9:25 – 10:10 AM	Turn 3 (Integrate)	Main table
10:10 – 10:20 AM	Break	
10:20 – 10:45 AM	Turn 4 (Assess / Discuss)	Discussion table
10:45 – 11:30 AM	Turn 4 (Integrate)	Main table
11:30 – 11:40 AM	Postevent Survey Questions	DECIDE®
11:40 AM – 12:00 PM	AAR / Closing Comments	Main table

Table 4: Schedule of Second ROC Drill

5.3. Event

Using the lessons learned from the Jack Pandemus exercise and the ROC Drills, the JV 3.0 exercises were conducted virtually for Charleston on September 22, 2020, and for Savannah on September 24, 2020. Because all participants logged in using different browsers from different locations around the country, with some participants logging in at home and others logging in from behind government or corporate firewalls, there were some technical issues with respect to logging in and seeing information presented in DECIDE®. Technical issues affected fewer than 10 participants per event and were resolved for all participants within 30 minutes of commencement. Having rehearsed event execution during the ROC Drills, the ACI was able to begin and end all turns within 1 minute of the planned times. Overall, execution of both events was smooth and efficient after the early-morning technical issues had been resolved. The event schedule is shown in table 5.

Time (EST)	Event	Location
8:30 – 8:50 AM	Welcome and Scene Setter	Main table
8:50 – 9:00 AM	Preevent Survey Questions	DECIDE®
9:00 – 9:30 AM	Turn 4 (Assess / Discuss)	Discussion table
9:30 – 10:15 AM	Turn 4 (Integrate)	Main table
10:15 – 10:25 AM	Break	
10:25 – 10:55 AM	Turn 5 (Assess / Discuss)	Discussion table
10:55 – 11:40 AM	Turn 5 (Integrate)	Main table
11:40 AM – 12:40 PM	Lunch Break	
12:45 – 1:15 PM	Turn 6 (Assess / Discuss)	Discussion tables
1:15 – 2:00 PM	Turn 6 (Integrate)	Main table
2:00 – 2:10 PM	Break	
2:10 – 2:40 PM	Turn 7 (Assess / Discuss)	Discussion tables
2:40 – 3:25 PM	Turn 7 (Integrate)	Main table
3:25 – 3:35 PM	Postevent Survey Questions	DECIDE®
3:35 – 4:00 PM	AAR / Closing Comments	Main table

Table 5: Event Schedule

5.3.1. Event Participants

In addition to the White Cell, many organizations with varying roles and responsibilities participated in JV 3.0: city management, city and county emergency management, port authorities, county school districts, fire and police departments, utilities, railway companies, the National Guard, several federal agencies, as well as others (see Table 1, "JV 3.0 Participants," in section 4.6). Some of these organizations communicate and depend on each other's services regularly, even daily, while others may never work together except in a crisis. These dependencies and interactions—or lack thereof—were a focus of the JV 3.0 exercises.

Participants were provided with and asked to abide by the *Jack Voltaic 3.0 Player Handbook*, which contained standards, guidelines, and instructions geared toward attainment of the event goals and objectives. To facilitate realistic participant responses to the scenario, the ACI established certain expectations. Participants were asked to accept the scenario events at face value, rather than questioning or fighting the "facts." Participants were asked to represent their organizations or sectors and react—given their existing capabilities, resources, and plans—as if the scenario were an actual incident. They were asked to execute their organizations' crisis action or incident response plans and to note any gaps in processes or procedures as well as identify necessary internal and external resources. They were also asked to identify the limits of their decision making and the decision making of superiors and subordinates. Participants were encouraged to stay engaged and use the exercise as a learning opportunity, voicing opinions, discussing options, and highlighting opportunities for improvement.

5.3.2. Group Interaction

Interactions between the White Cell and the participants were limited to the conversations led by the facilitator lead because any other conversations would not be properly captured, as required by the data collection and analysis plan. To protect the integrity and flow of the exercise, interaction between different participant groups was encouraged, but only if it was to coordinate or act in response to the scenario stimuli. Support staff were instructed to communicate only with the facilitator lead and exercise lead to ensure messages were coordinated and only coming from the ACI.

Prior to the start of JV 3.0, participants were directed to register for the event and set up a DECIDE® account. To start each exercise, the exercise lead welcomed participants, explained the goals of the event, and described how to use DECIDE® and Microsoft Teams. NUARI provided access to the DECIDE® exercise environment, and the White Cell and participants accessed both DECIDE® and the applicable Microsoft Teams meeting rooms. The facilitator lead explained the plan and schedule for the day, instructed participants to begin turn 4 by moving to their respective tables within Microsoft Teams, instructed the DECIDE® controllers to populate the turn injects in the DECIDE® platform, and set the time for all participants to return to the main table.

5.3.3. After Action Review

Upon completion of the exercise, the facilitator lead led an After Action Review discussion at the main table focused on overall thoughts about the day's events. Specifically, discussion centered on whether the exercise generated a better understanding of the possible risks and threats arising from a cyber incident, the players in the environment and their roles, and what the path forward should be. The purpose of this final discussion was to achieve a holistic assessment of the exercise and obtain recommendations for moving forward. Participants were instructed not to replay each event or to blame or otherwise attribute issues to specific organizations or participants; rather, they were asked to provide lessons learned, identify specific problems or issues, and recommend improvements. Finally, participants were asked to provide After Action Review comments in DECIDE®.

The initial feedback on JV 3.0 was primarily positive. Most participants thought the exercise was implemented effectively, despite COVID-19 causing the ACI to truncate and modify the event. The planning meetings and drills leading up to the exercise were recognized as having been very helpful.

As virtual meetings become more commonplace, many organizations struggle to adapt. To be successful, JV 3.0 required interaction among many different organizations of various types, whether they were private, public, federal, state, or local. Fortunately, the extensive planning and practice that the ACI conducted prior to the event proved to be both constructive and worthwhile.

Additional feedback and lessons learned can be found in chapter 6, "Findings."

5.4. Post-Event

In the weeks following the JV 3.0 exercise, the ACI planners hosted a series of out-briefings with partners and participating organizations. The initial feedback on JV 3.0 was primarily positive. After participants had had time to reflect, they provided additional insights on the usefulness of the exercise and its potential moving forward. Notes taken during these conversations contributed to the findings located in chapter 6 of this report.

5.5. Executive Out-Brief and Discussion

Due to the virtual execution of the event, the ACI converted DV Day to a 90-minute Executive Out-Brief. Held virtually on September 30, 2020, the ACI's intent for this event was to provide an effective forum for informing and engaging public and private senior executives about the outcomes and lessons learned from the JV exercise.

In addition to describing JV 3.0 and its participants, the ACI shared the following initial observations and corresponding strategic implications for planning, preparation, execution, and resources:

- Although many organizations are effective at dealing with natural disasters, many are not as prepared for cyber or information attacks. The interdependencies among sectors result in risks being shared by all; thus, everyone should review assumptions and adjust cyber incident response plans to improve resilience against potential cascading effects. Through increased information sharing and maintaining cross-sector partnerships, cities and private industry can achieve improved resilience through a whole-of-community approach.
- JV 3.0 did not directly impact telecommunications. Redundant communication channels should be developed and readied for degraded operations.

- The GA Emergency Management and Homeland Security Agency and SLED were very effective at bringing all of the incident response issues together.
- JV 3.0 highlighted the increased needs of states, cities, and the private sector for trained cybersecurity personnel and funded programs. Training opportunities should be increased, technology enablers leveraged, and repeatable frameworks developed.

Some highlights of the executive response included the following:

- It was widely agreed that JV 3.0 was a unique and timely exercise.
- Regarding the JV 3.0 scenario, one DV said it was appropriate to have cascading events rather than one catastrophic one because having numerous, smaller events forces players to identify thresholds for when to recognize purposeful threats.
- Recognizing the value in developing and maintaining cross-sector and cross-jurisdiction relationships to encourage a whole-of-government/whole-of-community approach, some DVs noted existing partnerships and connections that could be leveraged.
- The DVs recognized misinformation, disinformation, and the distortion of information as increasingly prevalent threats and emphasized the need to fill resource gaps to combat these threats.
- There was widespread agreement that the ACI and other cybersecurity and national security organizations should continue to hold exercises like JV and continue focusing on including state and local representatives in these valuable efforts.

6. FINDINGS

6.1. Examine the Impact of a Cyber Event on Army Force Projection

Though scenario injects focused on roadway congestion, rail delays, physical security considerations, communication with local authorities, and direction from higher headquarters for redirecting cargo, JV 3.0 illustrated how a cascading set of "below the threshold of armed conflict" events could disrupt local transportation unit operations involving these sectors. The effects of concurrent emergencies and cyberattacks on critical infrastructure owned by municipal, state, and private sector organizations could create conditions that cause force deployment and projection operations to halt, introducing a crucial decision point about whether to close the port or potentially divert deploying unit personnel and equipment elsewhere.

6.1.1. Findings

1. **The Army relies on various interdependent critical infrastructures, the majority of which it does not own or operate, making its domestic operations heavily reliant on external resources.**

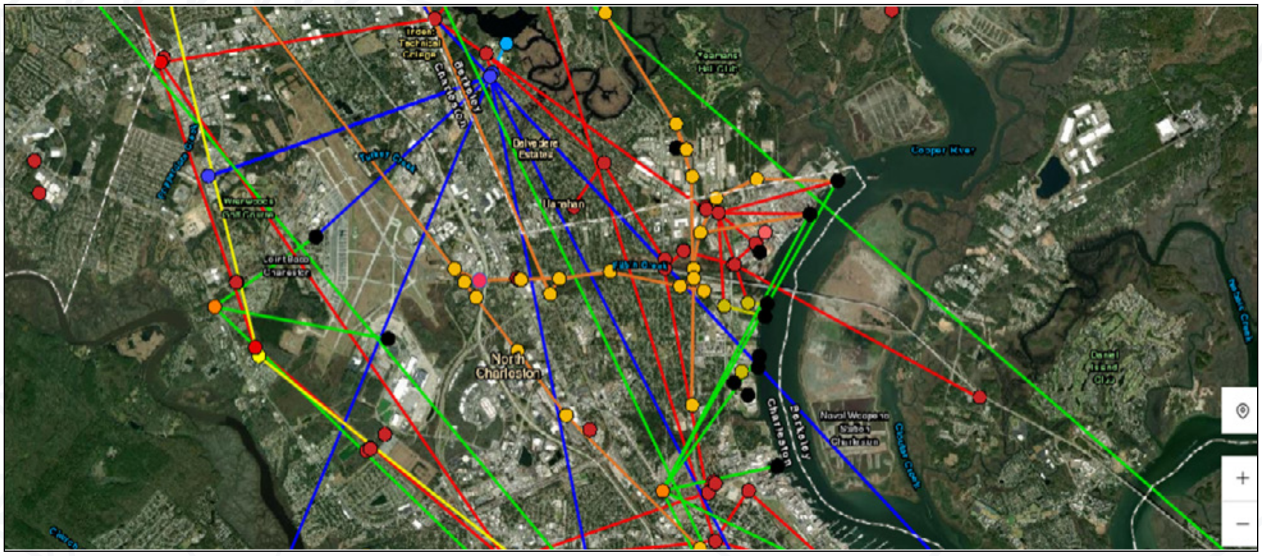


Figure 8: All Hazards Analysis (AHA) Dependency Model for the Transportation Sector—North Charleston

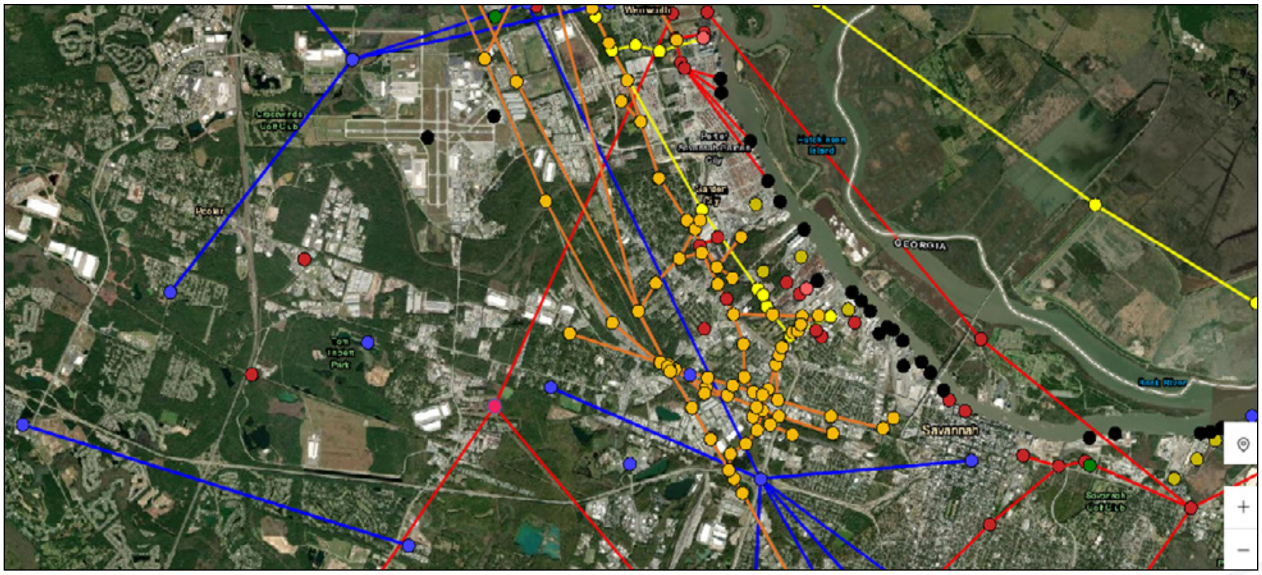


Figure 9: All Hazards Analysis (AHA) Dependency Model for the Transportation Sector—Savannah

a. Army transportation units responsible for moving, deploying, and sustaining combat power are reliant on both public and private critical infrastructure sectors, including energy (power), transportation (ports, rail, and road), and communications, that together enable the success of the units' mission. The interdependencies between these different sectors has the potential to create a set of complex and unanticipated challenges for these units and their mission. Figures 8 (North Charleston) and 9 (Savannah) show the All Hazards Analysis (AHA) dependency models for the transportation sector (see appendix H). In both figures, we see how electricity (red points and lines), natural gas (yellow points and lines), water (blue and light-blue points and lines), and communications (orange points) support and interact with port facilities (black points) and the rail network (orange lines). The JV 3.0 exercise showed how cyber or physical events that impact a single sector can generate cascading effects across interdependencies and introduce unplanned decision points for unit leaders.

b. Each port authority determines access to terminals and works with the United States Coast Guard (USCG) to determine the extent to which the port remains in operation, depending on the type and severity of incidents. In both the Charleston and Savannah events, the captains of the ports closed the ports pending the investigation of issues and the cleanup of cargo containers being dumped into the channel.

c. Rail companies have the final say in determining alternate routes for cargo in the event of redirection or recontracting. Trucking companies are another option for the movement of cargo, but the number of available drivers required to move a significant number of containers may exceed the capacity available locally.

d. Both ports and the surrounding areas use all forms of major commercial transportation to move to and from the port. Though this event included trucking and rail, it did not discuss the role of surrounding airports in movement to and from the ports.

2. **A sophisticated adversary can disrupt force deployment and cause units to miss the Required Delivery Date (RDD) by targeting commercially owned critical infrastructure and local municipal sectors.**
   a. During the scenario, the movement of military equipment was disrupted by a combination of traffic delays; social media-incited protests; port access manipulation; the manipulation of rail and vessel cargo manifests; natural gas and electrical disruptions; and, ultimately, interference with the weight distribution for the automated load plan for a ship in port, causing it to tip and dump containers into the channel.
   b. The only military infrastructure directly targeted in the scenario was SDDC email accounts. However, there was no significant escalation resulting in apparent disruptions that would cause excessive resource allocation. The Emotet malware's automated propagation caused this compromise, but there was virtually no conversation about this particular thread, and it was never intended to be a primary concern.
   c. In the scenario, a brigade-sized armored task force consisting of approximately 2,300 pieces of equipment was tasked to conduct a rapid deployment to a theater of operation. Using the movement from Defender 2020 as a template for the JV 3.0 scenario, the movement of this equipment to the port would require four trains with 50 cars apiece, 100 to 150 trucks, and 20 serials of military convoys. As a result of cyber incidents during the scenario, approximately 280 pieces would have been delayed or stopped upon the closure of the port at the end of turn 5:
      i. Two trains with 120 pieces of cargo, with the possibility of delaying or stopping two more trains;
      ii. Twenty to 40 trucks with 100 total pieces of cargo; and
      iii. One serial of a military convoy with 60 pieces of cargo, with the possibility of delaying more.
   d. The ACI and its partners developed a Monte Carlo simulation to analyze potential alternatives for the commander (details on the simulation are found in appendix J):
      i. Remain at the original port until it remediates physical and cyber issues (at the end of turn 5, a cargo ship listed and dumped containers into the channel);
      ii. Assume there are no issues with the channel and remain at the original port until it remediates the cyber issues;
      iii. Relocate to a new port 200 miles away; and
      iv. Relocate to a new port 1,000 miles away.
   e. The goal of the simulation is to generate a distribution that represents the number of days required to complete the force projection operation, and then develop probabilities associated with successfully making the original RDD of June 1, 2020 (complete movement in 28 days or less). For the alternatives analyzed, remaining at the original port provides commanders the best probability of arriving by the original RDD (23-percent chance of successful completion in 28 days when required to clear the channel and 77-percent chance of successful completion when there are no issues with the channel). Even with a significant physical effect (blocked channel), the alternatives that involved moving showed much less promise. For these alternatives, the time is dominated by recontracting and replanning for the new port (moving to a new port 200 miles away has a 1-percent chance of successfully making RDD). Appendix J provides more information on the simulation.

3. **A sophisticated adversary can disrupt deployment and cause units to miss the RDD by using cyber capabilities that do not trigger an armed response but still achieve cascading effects that complicate a coordinated response.**

    a. No one scenario event seemed challenging enough to prevent a force projection operation from achieving its RDD. These delays, though, negatively impact the marshaling of space and load planning at the port of embarkation. Although it is possible to load vessels with equipment that has arrived at the port staging areas, the delays impact load planning (by both the military and contractors) that would likely decrease the operational capability and capacity of elements when they arrived in their designated theater of operations. Geographic combatant commanders and their subordinate task force commanders would likely require significant operational plan modifications to meet impending deadlines due to these force packages being disrupted at the port of origin and the intended port of debarkation. The decision to ultimately divert equipment and personnel to an alternate port of embarkation creates additional timing concerns regarding expected arrival times within a theater of operation; these concerns include, but are not limited to, convoy security, personnel availability, return, remarshaling, and departure to an alternate port.

    b. The Emotet cyber tool was the chosen malware tool for the JV 3.0 scenario due to its availability and annual release since 2016.[22] The Planning Team chose events for the scenario that mirrored real-world incidents in which it was unclear whether the actors were nation-state operatives.

    c. Using inject distribution directed by DECIDE®, participants faced a situation with imperfect information. The deliberate nature of inject escalation allowed each sector to handle initial incidents with ready resources and known agreements. Soon, however, participants acknowledged service disruptions were leading to overwhelming downstream effects on other sectors. In both cities, once participants acknowledged that the scenario events were clearly indicating a coordinated cyberattack by an unknown adversary beyond their ability to manage, they shut down the ports indefinitely. The closing of the ports pushed SDDC to identify alternative means of force projection.

    d. During execution, participants avoided discussion about attribution because it was not clear to them that the incidents had been caused by cyberattacks, much less a sophisticated adversary. By the time the players were willing to state that the set of incidents was a coordinated effort, the damage was extensive and attribution was highly unlikely.

4. **Interactions and interdependencies between communications and information technology (IT) systems present new gray-zone attack vectors that can have debilitating impacts on Maritime Transportation System (MTS) operations vital to force projection.**

    a. The UIUC CIRI Port Disruptions Tool (PDT) simulation (see appendix I) used incidents consistent with the injects in JV 3.0 to demonstrate the potential impacts of fort-to-port, communication-based disruptions on force projection.

    b. A train derailment due to compromised rail-control signals introduces a minimum 2-day disruption that requires significant coordination and reallocation of resources for mitigation and response (see disruption 1 [D1] in appendix I). The challenges associated with mitigation include the location of the derailment (more complex in an urban environment as opposed to a rural one), the impact of rerouting rail and road transportation movements, and the speed with which additional movement assets can be acquired. Furthermore, any change to the arrival schedule for the equipment will impact gate usage at the port as well as vessel loading.

[22] Bromium, *Emotet: A Technical Analysis of the Destructive, Polymorphic Malware* (Cupertino, CA: Bromium, 2019); and “Alert (TA18-201A): Emotet Malware,” United States Computer Emergency Readiness Team, updated January 23, 2020, https://us-cert.cisa.gov/ncas/alerts/TA18-201A.

c. The increased use of digital communications by railroad companies introduces the potential to delay rail by degrading the communication network (see disruption 2 [D2] in appendix I).[23] In this situation, route choice may also affect the exposure of data to adversaries, depending upon the communications networks utilized. Exposure to unmanned aerial vehicle-based (UAV-based) man-in-the-middle (MITM) attacks may be worse in rural areas, where railroad companies rely on wireless networks, and technologies may enable one to use MITM methods to access operational data via cell phone signals used by emerging applications employed by rail companies.

d. Rerouting traffic can result in new single points of failure across multiple critical infrastructure sectors (see disruption 3 [D3] in appendix I). Planners must recognize emerging risks due to the data or stakeholder dependencies of secondary and tertiary routes and time delays caused by disrupted movements.

5. **The current multidomain environment becomes contested for deploying units as early as the fort, thereby presenting the potential for degraded freedom of maneuver when conducting home-station movement operations. Therefore, military deployment operations can no longer assume such favorable conditions and must plan and prepare for and be ready to mitigate such physical and cyber disruptions accordingly.**

a. Cascading cyber and physical incidents introduce several interrelated complexities that both local garrison commands and municipal emergency operations centers must be made aware of early due to mutual dependence on supporting critical infrastructure, such as energy (power), transportation (ports, rail, and road), and communications (telecommunication).

b. JV 3.0 exercise data highlights a gap in early indications and warning that leaves local garrisons unaware of initial cyber intrusion impacts across interdependent critical infrastructures. This observation further exposes the importance of:

i. Codified relationships between garrison emergency operations centers and civilian municipal entities;

ii. Established information sharing between emergency operations centers that communicate early and often when large ground convoys are traversing to or from ports of embarkation;

iii. Awareness of the availability of critical resources (and the entities from which these resources are available) to support mutual rerouting or cross-loading during such scenarios; and

iv. The establishment of multidomain protection protocols for all moving stock and associated personnel (military and civilian) transiting between installations and ports through mutually reinforcing agreements and relationships.

c. JV 3.0 interactions revealed that when responding to multiple events, garrison commands are continuously faced with taxing constraints that may divert critical resources and exceed maximum thresholds. This observation necessitates:

i. Designing, establishing, exercising, assessing, and codifying support structures among garrison, local, state, and regional emergency management, cyber incident response, and critical infrastructure partners.

ii. Establishing communication protocols among brigade, division, and garrison transportation offices along with SDDC, United States Transportation Command (USTRANSCOM), and

[23] Angela Cotey, "Railroad Communications Technology: From Cellular to Radio to Satellite to Wi-Fi," *Progressive Railroading*, May 2012, https://www.progressiverailroading.com/norfolk_southern/article/Railroad-communications-technology-from-cellular-to-radio-to-satellite-to-Wi-Fi--30947.

municipal emergency service stakeholders when planning, preparing, and deploying unit convoys to and from ports of embarkation.

iii. Creating a common operating picture among local garrison, municipal, state, regional, and private sector partners with interdependent critical infrastructures to mitigate the disruption of departing convoys—a scenario that can present operational impacts across multiple domains.

d. Installation response plans, procedures, and protocols require additional development to ensure both a holistic response and the continuation of movement when garrisons are presented with emergency and cyber incidents that cascade across interdependent critical infrastructures. This observation further highlights:

   i. The increasing feasibility and likelihood that garrisons will face a JV-type, complex, cyber and physical incident and not be structured, equipped, resourced, or prepared to adequately ensure sustained installation unit survivability and resilience.[24]

   ii. The criticality of garrisons receiving early warning from both public and private sector partners at the first indication of a developing incident that has the potential to result in debilitating effects (both physical and digital) on deploying units.

   iii. The importance of implementing an agile and flexible incident response framework that best enables continuous communication, cooperation, and collaboration among garrisons and municipal and private sector incident response stakeholders (both cyber and physical).

6.2. Exercise the Cities of Charleston and Savannah in Cyber Incident Response

Through JV 3.0, the ACI introduced a series of workshops and an exercise that allowed the cities of Charleston and Savannah to examine, assess, and update their current cyber incident response procedures. Although both cities' capability to respond to natural disasters is very mature and well-rehearsed, incorporating a cyber element into the exercise provided an opportunity for the cities to rehearse their response plans; examine their protocols regarding cybersecurity; and improve communication within the cities, their departments, local critical infrastructure sectors, and regional organizations.

This was the first time that JV has looked beyond a single metropolitan area, exploring the similarities and differences between the laws, policies, and responses in two cities in the same region but different states. Originally intended to be conducted simultaneously and in parallel, COVID-19 forced the team to refocus efforts and conduct two identical scenarios one day apart. Both cities performed admirably through the planning process and exercise, with the research findings listed below.

6.2.1. Findings

1. **There is no standard for cyber incident declaration. Cyber incident declaration was found to be insufficient in addressing activities that are rated as below catastrophic and are likely not as obvious, yet are still operationally impactful for all parties.**

   During the TTX, the ACI observed a general reluctance of participants to openly declare a cyber problem existed or state the circumstances unfolding could be, or were, connected to a cyber event. Although participants knew this was a TTX with a cyber nexus, the physical impacts of

[24] Sydney J. Freedberg Jr., "Our Bases in US Will Be Attacked: Army," Breaking Defense, December 14, 2020, https://breakingdefense.com/2020/12/our-bases-in-us-will-be-attacked-army/?fbclid=IwAR36rBTp-z55DAwDJM8seCsLT2ep0WeO7HCH-l6NPnoOxctb70EsQpLkw9c, accessed January 5, 2021.

scenario events slowed the participants' engagement in areas that could be cyber-related and the subsequent identification of indicators of potential emerging issues. Although many participants and entities had response plans that included cyber incidents, participants demonstrated more clarity on response, protocols, and processes when addressing elements of the exercise that were physical in nature.

2. **There is an emerging need for city-level information security departments to address potential cross-system issues between organic and isolated networks, such as supervisory control and data acquisition (SCADA) and traffic management systems.**

   Organization leaders should understand that information security and IT are separate disciplines and should allocate resources accordingly. The growing number, variation, and interconnectivity of municipal IT and operational technology (OT) systems, networks, and structures necessitates a deeper analysis of potential cross-system connectivity to be able to adequately address the potential impacts of a cascading intrusion that maintains the propensity for the degradation of multiple critical infrastructure sectors simultaneously due to shared connectivity, hardware, and/or software. This cross-system analysis should consider the following:

   a. Review of all municipal agreements and contracts for the parameters of cyber incident response support from contracted vendors and firms;
   b. Examination of municipal continuity of operations planning for city data facilities during a long-term degradation of critical infrastructure services, such as power;
   c. Analysis of all upstream and downstream data transmissions to determine the potential for cascading impacts across multiple critical infrastructure sectors;
   d. Risk analysis of municipal critical infrastructure systems that necessitate the sharing of common hardware and software;
   e. Exploration of the potential for critical infrastructure system and network segregation when appropriate, feasible, and necessary to prevent widespread impacts of a cascading cyber incident;
   f. Research on how critical systems (such as fire department mobile data terminals) might be impacted by a complete communications blackout; and
   g. Analysis of how a complete communications blackout might affect municipal water and sewer resource networks, including SCADA and other critical systems.

3. **Participants across sectors and levels of government noted that the realistic scenario incidents stressed the participants' procedures and forced them to think differently.**

   Participants indicated through exercise survey responses that the presented scenario elements were realistic and comprehensively taxing for different sectors and entities and simulated the actual flow of an incident unfolding. Regarding scenario realism and the inducement of participant stress during the event, we asked participants to self-report stress levels after each turn. Accordingly, these data indicated that stress levels consistently increased from turn to turn as issues and challenges continued to cascade, with two-thirds of survey respondents indicating a high level of stress by the final turn of the exercise (see figure 10). This feedback indicates participants and their respective organizations felt enabled in implementing their respective incident response actions, and JV 3.0's bottom-up approach was informative and added value to participants' future decisions.

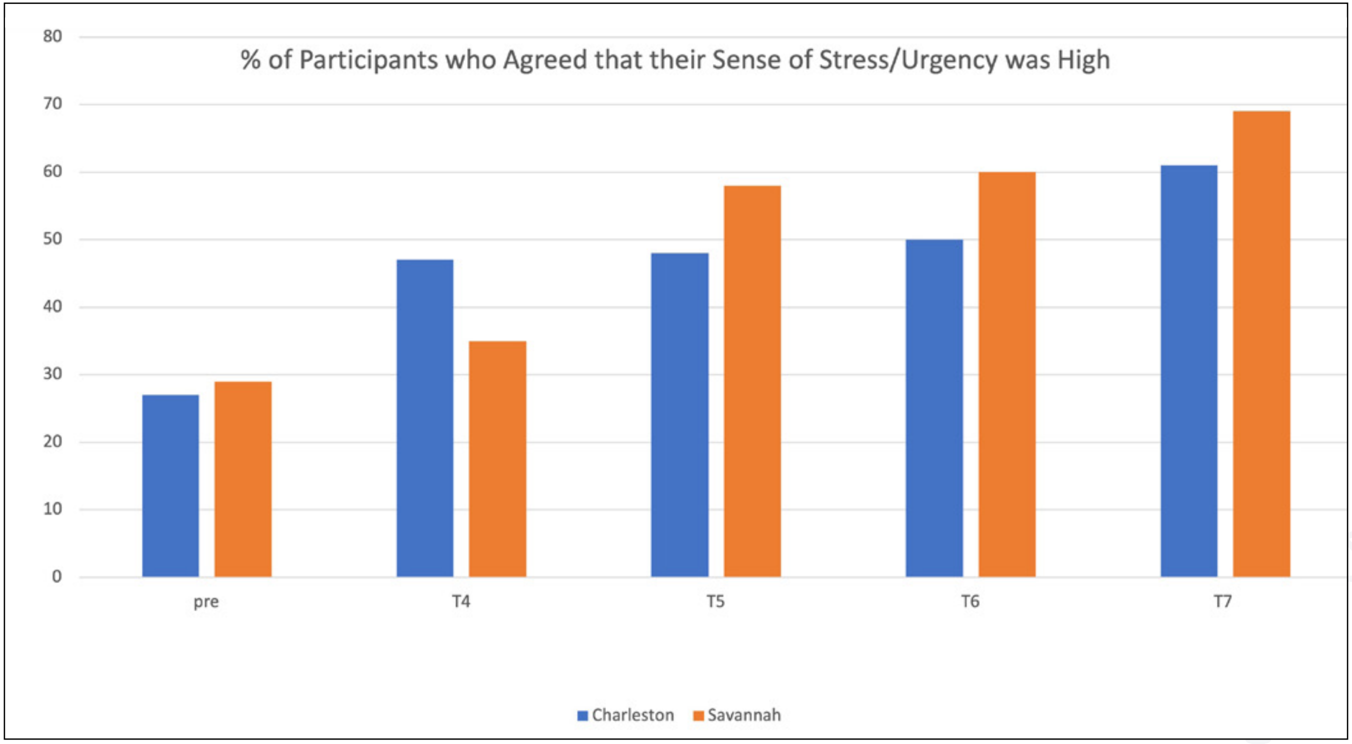


Figure 10: Stress of Participants by Turn

4. **Participants across sectors and levels of government should use municipality-focused cyber exercises to improve overall incident response.**

   In both JV 3.0 exercises, participants overwhelmingly indicated with 88-percent positive responses that the exercise provided them with new information or sources of information relevant to incident response, such as available resources, new knowledge on infrastructure and policies, and organizations that support community lifelines. Eighty-four percent of survey respondents also reported that JV 3.0 helped them identify gaps in their respective incident response plans regarding knowledge, resources, communication channels, and the commitment of personnel during incident response. Additionally, 83 percent of survey respondents reported that participation in JV 3.0 would help their organization improve its incident response plan going forward. Figure 11 further illustrates this point, with a majority of participant-driven measures being classified as either a communication (orange), action (red), or plan (brown) between organizations throughout both iterations of the event. These response percentages, coupled with corresponding observation data and testimonials, suggest that most participants felt that their time, energy, and resource commitment translated into added value for their organizations following JV 3.0.

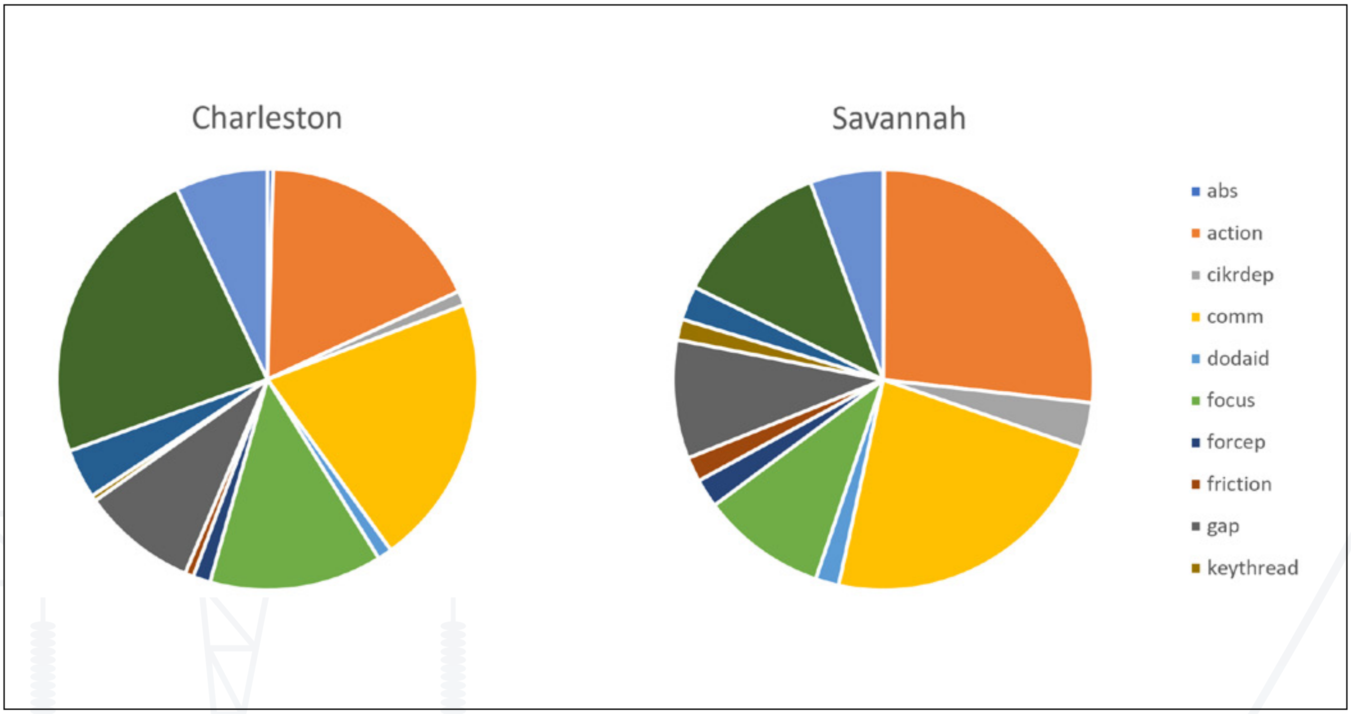


Figure 11: Participant-Driven Measures in the JV 3.0 Exercises

5. **Municipality-focused cyber and emergency management exercises can be effectively executed in a distributed format that supports continuous participant engagement across both public and private sector stakeholders.**

   JV 3.0 demonstrated that it is possible to effectively conduct an event that exercises incident response in a distributed manner, utilizing multiple facilitation platforms. Participant survey responses and testimonials overwhelmingly support this finding, with 86 percent of survey respondents reporting that JV 3.0 held their attention and kept them actively engaged for most of the event. Individual testimonials further bolstered this finding, with one participant stating:

   > *The Virtual means of delivery really shined [in including] everyone [as if they were] in one location. I believe that in an event of a real crises the need for IT system such as Decide in combination with MS TEAMS will really help facilitate communications, Corrective COA, and engagement from multiple personnel from multiple levels. I noticed everybody got to work simultaneously which I've never observed before.*

   The efficacy of this JV 3.0 distributed design also allowed additional entities, organizations, and individuals to participate that may not have otherwise had the ability to do so. Additional individual testimonials further reinforced this finding, with participants indicating that:

   > *Doing this virtually actually helped me participate as I don't know if I could have [gotten] away from the office to do this.*

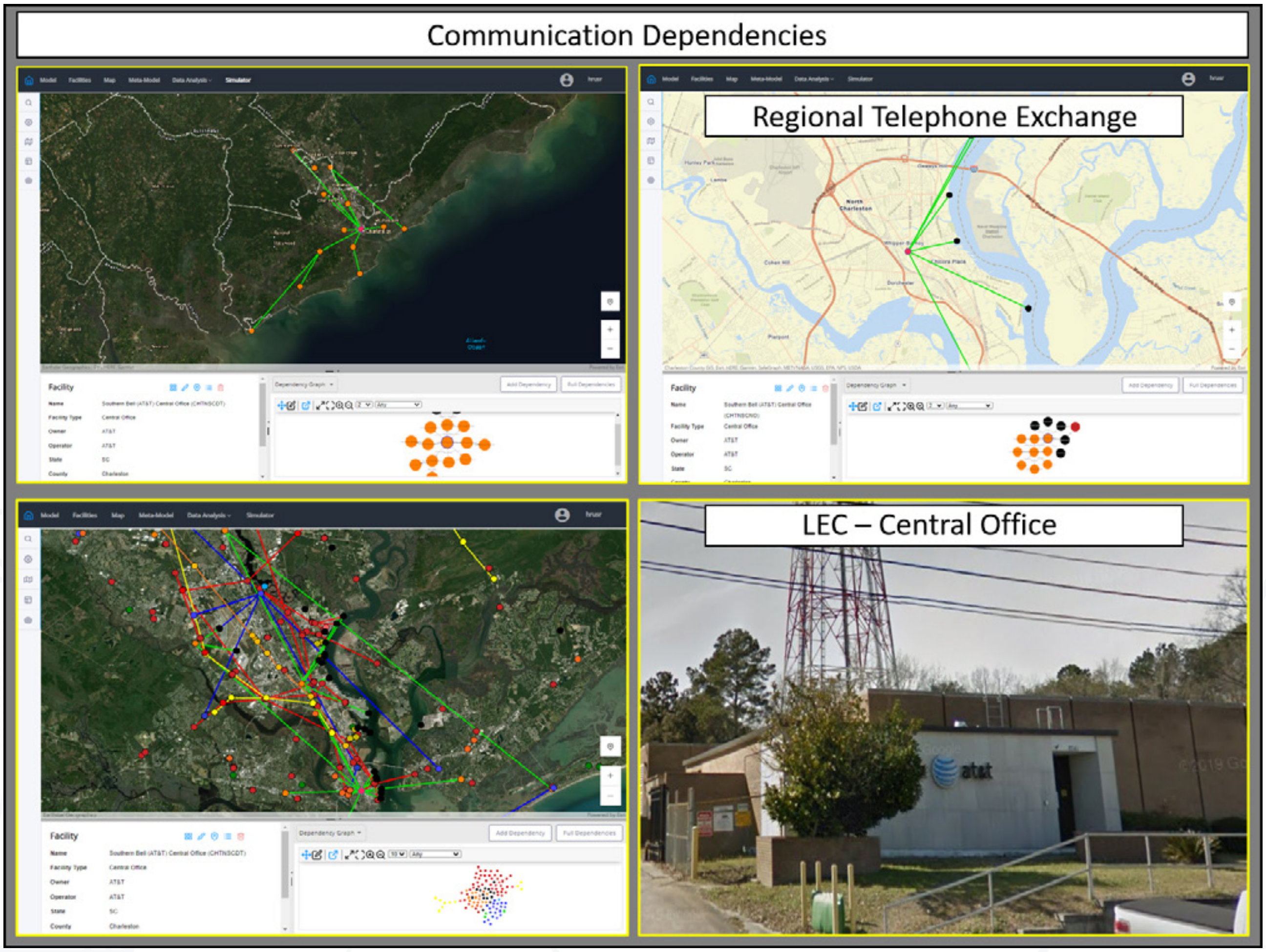
   > *Great job for taking this virtual and still having this be a productive exercise.*

This finding not only indicates the efficacy of this distributed iteration of JV 3.0, but also informs future research with respect to the creation of an automated JV platform in support of creating a repeatable and adaptable framework. The finding also suggests that there may be value in creating a virtual environment that supports multidomain collaboration when critical infrastructure organizations are managing cyber-physical incidents.

6.3. Reinforce a Whole-of-Community Approach

Whereas a whole-of-government approach is a culture that promotes information sharing, cooperation, and coordination of resources at all levels of government, the whole-of-community approach recognizes the physical and cyber interdependencies among all levels of government, private industry, and critical infrastructure sectors. Prior to the advent of cyberattacks, the United States could safely assume the civilian sector would operate smoothly in support of military and economic functions and its military dominance would protect domestic operations. Now, a clever adversary can use techniques and tools in cyberspace to exploit a host of seemingly minor interdependencies whose downstream effects will aggregate to a significant event.

There are relatively well-understood interdependencies among critical infrastructure sectors, such as natural gas and electric; power and water; and communications and ports, to name a few. To illustrate, figure 12 shows the AHA communication sector dependency model for major lifeline critical infrastructure (see appendix H). The upper-left quadrant shows communication dependency links (green lines) and communication facilities (orange circles), and the top-right quadrant adds nodes to indicate port facilities (black) and substations (red). The bottom-left quadrant shows the interdependencies that exist among electricity (red), rail (orange), natural gas (yellow), and water (blue). Given the multiple sectors included in the dependency model, it is imperative that local governments include as many critical infrastructure sectors in their cyber incident response plans, rehearsals, and exercises. Through the whole-of-community approach, we can identify where these interdependencies exist and take appropriate measures to ensure that incidents do not create cascading effects.



Facility
Name Southern Bell (AT&T) Central Office (CHTNSCDT)
Facility Type Central Office
Owner AT&T
Operator AT&T
State SC
County Charleston

Facility
Name Southern Bell (AT&T) Central Office (CHTNSCNO)
Facility Type Central Office
Owner AT&T
Operator AT&T
State SC

Facility
Name Southern Bell (AT&T) Central Office (CHTNSCDT)
Facility Type Central Office
Owner AT&T
Operator AT&T
State SC
County Charleston

Figure 12: Communication Dependency Model (Charleston)

Perhaps most importantly, the local and private entities that are exploited to cause cascading effects are the first on the scene to combat the adversary. As such, initial response activities may be dictated by nongovernmental agencies. Whole-of-government culture for cyber incident response is good but insufficient; critical infrastructure resilience requires a culture that embraces and mobilizes the entire affected community.

6.3.1. Findings

1. **Although traditional incident responses—such as for natural disasters or chemical or biological threats—are generally effective and coordinated, there is a need for improving responses to purposeful cyberattacks.**

   Cyber incident responses require rapid information sharing and requests for assistance from state and local players. Local events can have significant cascading impacts throughout the county, state, and Nation. Differences among city, state, federal, and private sector responses can add significant complexities. Thresholds for information sharing and reporting are critical to understanding situations and recognizing an attack. The exercise illustrated cases in which sharing and reporting did not happen in a timely manner or could not extend beyond an organization, thus preventing the early identification of a cyber incident. Also, gaps in understanding the chain of authority for requesting additional resources can impact requests for and the deployment of state and federal assistance.

Furthermore, differences among city, state, federal, and private sector incident responses and levels of transparency are not necessarily conducive to trust or situational awareness. Evidence from JV 3.0 clearly illustrates that different levels of government and different sectors have different perspectives, and each agency or level may only see part of the whole picture. After receiving the incident injects for each turn, the participants discussed the new or ongoing issues that were most relevant and pressing to their respective sectors; this information was tracked by data collectors using the data code "focus." The word clouds in figure 13 illustrate that different tables (sectors) focused on different aspects of the situation. For example, the city table focused strongly on local traffic issues and, to a lesser extent, issues related to students (who were impacted by water supply issues at the schools). A key focus of the port table was a combination of power disruption issues related to protestors, continuity of operations, and potential impacts on the port's military customers. The energy sector focused on responding to ransomware, maintaining its services for the business sector, and potentially leveraging third-party vendors to compensate for shortfalls. The federal/military sector reflected "cyber" as a front-and-center focus (though the word "ransomware" is in the word clouds for the other three sectors pictured).

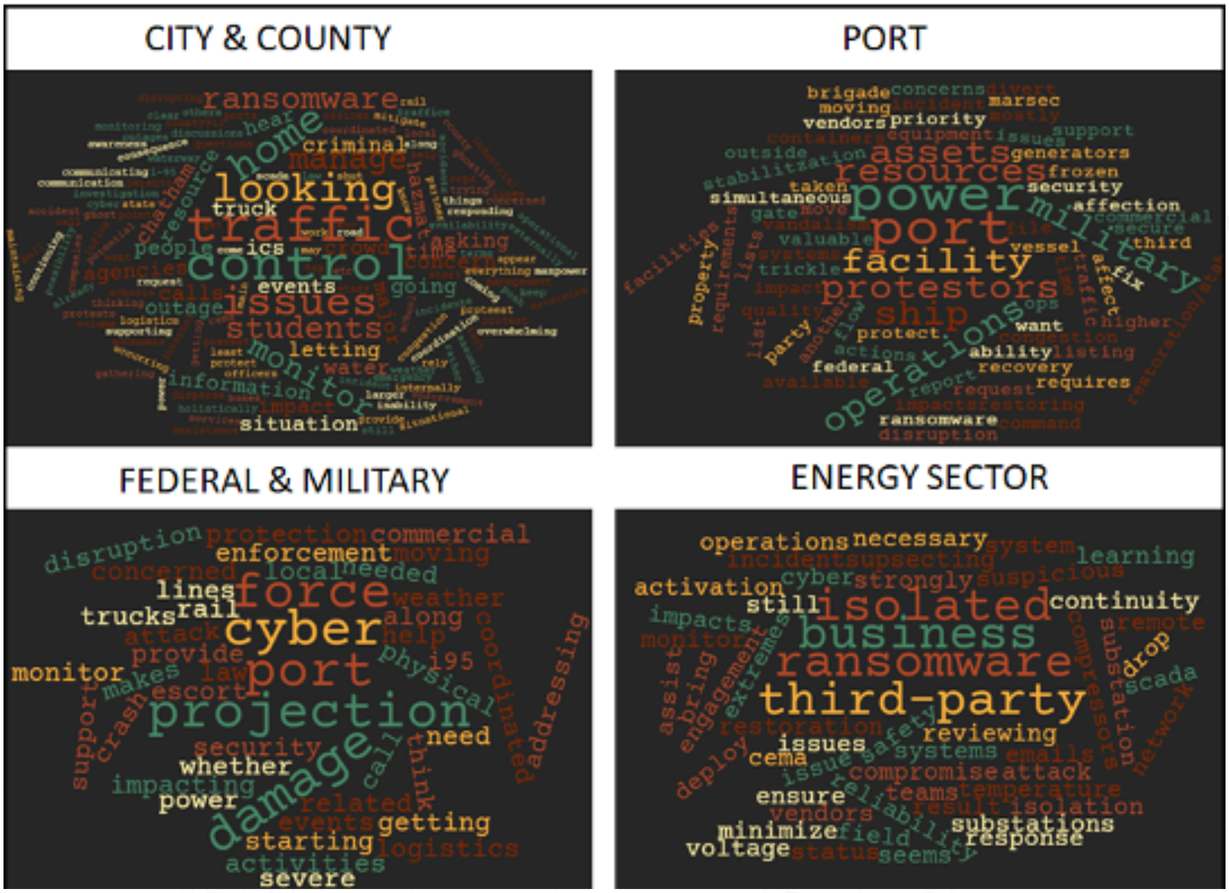


Figure 13: These word clouds illustrate that different sectors had different perspectives, focused on different aspects of the situation, and allocated different weights to common issues.

2. **JV 3.0 addressed the need of many participating agencies affiliated with the cities for fully formed response plans and communication networks.**

   From a whole-of-community perspective, JV 3.0 demonstrated it is possible to bring critical public and private sector stakeholders together in the same exercise. Many exercises present notional injects that do not necessarily pertain to stakeholders' organizations, sectors, or spans of responsibility. Though this approach helps maximize resources, it fails to bring the full complement of required participants to the table, a practice that distills interdependencies and gaps in cyber incident response. This need was identified by roughly half of survey respondents, who stated that they did not yet have a good awareness of how different organizations or sectors in their cities (and beyond) would communicate and coordinate during a cyber incident involving critical infrastructure. Although larger exercises come at a cost, participants desire to gain more situational awareness about the processes used across organizations. Some of the JV 3.0 participants' expressed goals included the following:

   a. *"[To] better understand how the state and federal agencies work together for a non-[Department of Defense] cyber incident."*

   b. *b"[To achieve] better understanding of how state, local and commercial entities would respond in a crisis situation. At what point would this individual event be reported up to the Federal level."*

   c. *"[To] learn from other partners to gain knowledge on if and where . . . we fit into their plans."*

   d. *"[To] find out how to contact and utilize exterior assets during a cybersecurity attack."*

   e. *"[To] learn who I'd reach out to [outside of my organization] in the event of a cyber crisis." Consequently, although a clearer understanding may exist at the state and federal levels, JV 3.0 highlights the desire for better understanding, knowledge, and integration at the municipal level—particularly, how to request assistance during cyber incident response.*

3. **JV 3.0 revealed the need for more regular and codified cross-sector communication and collaboration efforts during cyber incident response.**

   As mentioned earlier, JV 3.0 demonstrated an ability to bring stakeholders from various organizations and with different roles together under the auspices of a single cyber-physical critical infrastructure exercise. At the city level, there was a clear recognition of the need to conduct follow-on exercises that include multiple stakeholders to identify gaps in their cyber incident response plans, capabilities, and response actions across each community.

   Communication network visualizations generated from the exercise data further illustrate the cross-sector collaboration efforts that were initiated during JV 3.0 due to various exercise elements being introduced within the scenario. Figure 14 is an illustration of scenario-induced cross-sector communication by exercise turn that took place during JV 3.0, with the port depicted as the center of gravity. Though the port is depicted as communicating with traditional maritime stakeholders, this visualization demonstrates increased coordination with new municipality, county, state, federal, and private sector stakeholders during response efforts as well.

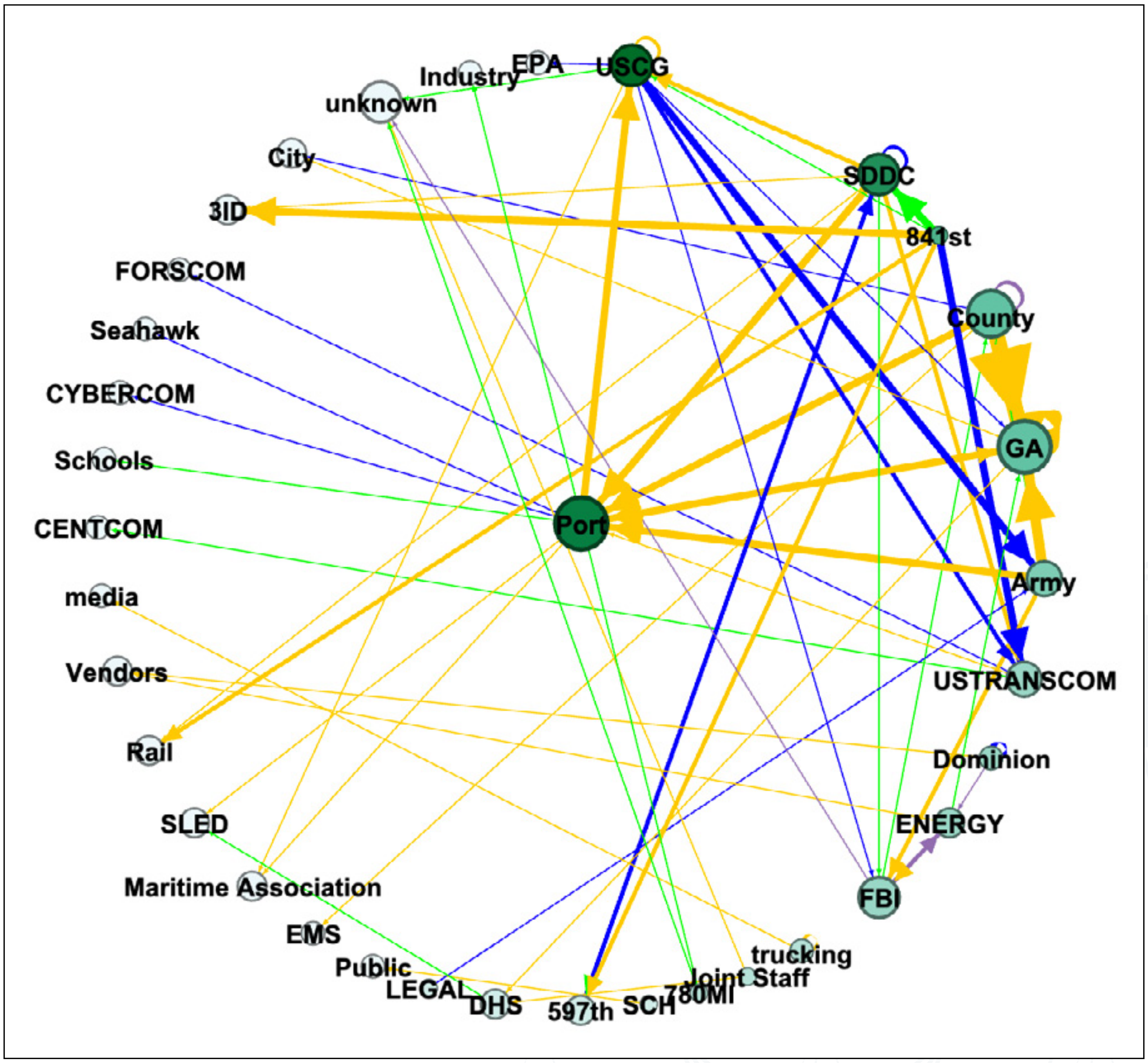


Figure 14: In this snapshot visualization, the organizational nodes representing different agencies are sorted in clockwise order by the number of requests they made to another agency. The more requests the agency made, the darker the color. In addition, the larger the node, the more requests the agency received. The colors of the edges represent the turns in which the relationship occurred: orange for turn 4, green for turn 5, blue for turn 6, and purple for turn 7.

A municipality's well-established and well-developed relationships with local stakeholders, both public and private, as well as effective internal communications and response actions are key strengths that can be leveraged during cyber incident response. Accordingly, JV 3.0 highlighted the value of further expanding cross-sector communications, plans, and cooperation, which can lead to earlier identification and consistent engagement with additional community partners—private industry, utilities, state entities, federal partners, and military installations—and thereby improve the speed, agility, and effectiveness of whole-of-community cyber incident response. Participant testimonials and survey responses underscore the importance of these scenario-induced cross-sector communications.

   a. “Many issues were identified that were very relevant, especially in the areas of determining when agencies would actually talk to each other, and if we were even speaking the same language.” —City participant

      i. According to survey responses, scenario incidents prompted over half of participants (in both iterations) to contact (or want to contact) another organization at some point in the exercise, and approximately 20–30 percent of respondents signaled they reached out (or wanted to reach out) to an external organization during each turn of the event scenario.

4. **JV 3.0 and the JV series continue to facilitate lasting relationships between a vast array of participating organizations, entities, and sectors.**

   JV 3.0 planning, design, and execution afforded a multitude of participants various opportunities to interact, collaborate, and integrate cyber incident response efforts for the first time. Accordingly, participation in planning conferences, workshops, and mini-exercises (Law and Policy TTX / Jack Pandemus) enabled stakeholders to further codify and incorporate these new relationships in advance of event execution. This sentiment continued into event execution, with approximately 90 percent of survey respondents requesting that their contact information be shared with fellow participants to facilitate ongoing communication and coordination for postevent incident response. JV 3.0 brought numerous public, private, federal, and academic stakeholders together for the better part of 15 months, facilitating the creation of these vital relationships that remain critical to bolstering whole-of-community critical infrastructure resiliency when faced with cascading and cyber incident emergency situations.

5. **JV 3.0 successfully brought together a wide array of public, private, military, and academic stakeholders during event planning, preparation, and execution for the first time. However, the consensus remains that these new relationships must be continually fostered, and additional stakeholders (those who did not participate in this iteration of JV) must be both identified and incorporated going forward through future, organically driven, JV-like efforts.**

   Municipal governments were the critical node for the JV bottom-up approach to increasing the resiliency of U.S. critical infrastructure. This iteration of JV continuously sought to facilitate a more robust whole-of-community response through the creation of new relationships, robust partnerships, and integrated joint response efforts. Although this was achieved to a great degree during JV 3.0 and fostered throughout its supporting events, efforts should be made to maintain these relationships while incorporating new and emerging stakeholders. This finding became clear when analyzing city-based communications following JV 3.0; it was evident that a concerted effort (driven by local communities) must be made going forward to continually strengthen and foster these new relationships, partnerships, and joint incident response efforts. Figure 15 is an illustration of emerging communication channels between the city and other important community stakeholders that began to take shape during JV 3.0. However, this graphic also depicts a need for further development, exercising, and codification of these new relationships not only with the participants that were present during this iteration, but also with additional stakeholders yet to be identified through future efforts that can continue to fill identified community gaps in resources, capabilities, and communication channels.

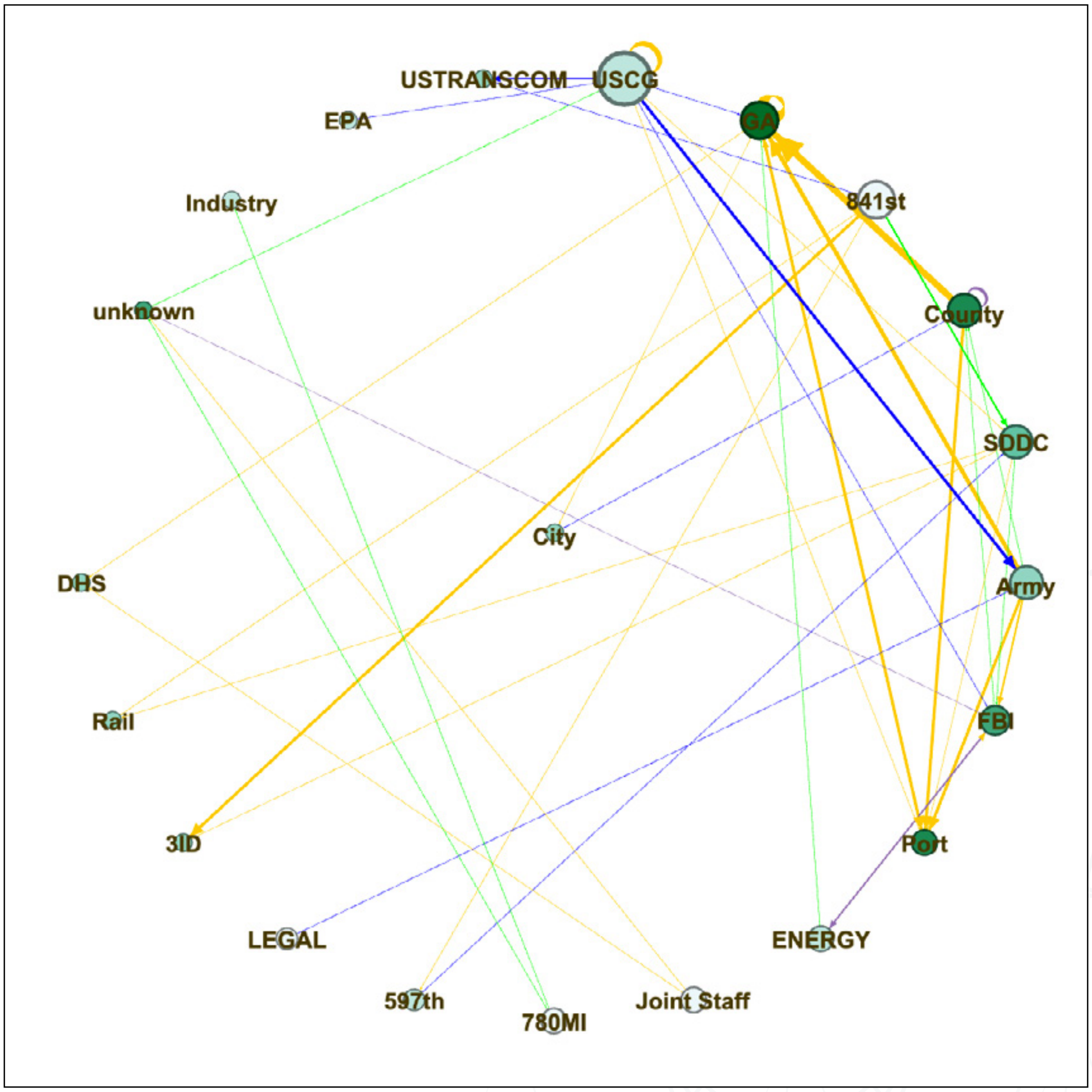


Figure 15: In this snapshot visualization, the organizational nodes representing different agencies are sorted in clockwise order by the number of requests they made to another agency. The more requests the agency made, the darker the color. In addition, the larger the node, the more requests the agency received. The colors of the edges represent the turns in which the relationship occurred: orange for turn 4, green for turn 5, blue for turn 6, and purple for turn 7.

6.4. Examine the Coordination Process for Providing Cyber Protection Capabilities in Support of DSCA

Based on the deputy secretary of defense's Directive-Type Memorandum 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response*,[25] the ACI refers to Defense Support of Civil Authorities (DSCA) / Defense Support to Cyber Incident Response (DSCIR) to achieve effectiveness in coordinating responses to significant cyber incidents.

[25] Robert O. Work, *Interim Policy and Guidance for Defense Support to Cyber Incident Response*, Directive-Type Memorandum 17-007 (Washington, DC: Office of the Secretary of Defense, updated May 29, 2020).

Though multiple agencies may be involved in the response, typically the Department of Homeland Security (DHS) or the Federal Bureau of Investigation (FBI) operate as the federal lead agency for threat response activities. More specifically, the Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities; DHS, acting through the National Cybersecurity and Communications Integration Center, is the federal lead agency for asset response activities; and the Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the federal lead agency for intelligence support and related activities.

6.4.1. Findings

1. **Though DSCIR has been codified in policy, it has not yet been exercised, and it is unclear how it would work during an incident.**
   a. The Law and Policy TTX included a separate forum for federal, state, and local government representatives to discuss the process for local municipal and state governments to request support in the event of a cyber incident. The organizations that attended this and other workshops included both prospective requestors and providers. Prospective requestors did not know whom to contact or what the process for requesting assistance was, almost without exception, and were usually surprised when representatives from prospective providers identified themselves. Although JV allowed for these introductions, repeat examples underscore the division between those with resources and responsibilities to help and those who will need it when their own resources are overtaxed.
   b. Many of the triggers for the release of resources are contingent on the declaration of a cyber incident, thereby delaying any possible DSCIR requests—assuming that participants know how to initiate them. When anomalistic behavior occurs, users tend to view it as a glitch or fluke and to attempt to restart or even replace systems. An adversary can exploit this by making cyber incidents ambiguous, increasing the time from discovery of the problem to cyber incident declaration.
   c. In the event of a cyber incident at the municipality level, stakeholders would have to notify their respective states and/or the lead federal agency for the critical infrastructure sector involved. Once notified, the lead federal agency would be the entity responsible for requesting DoD support. Though the request process had happened multiple times, DSCIR support had not yet been executed by the Law and Policy TTX in February 2020. Two main drawbacks to DSCIR support are the time required to process the request and send support and the cost of support.
2. **DSCIR should provide a menu of options and their associated costs similar to DSCA's menu of physical assets.**
   a. JV showed that malicious actors can cause a series of minor disruptions and escalations that can cascade into a significant disaster. By overtaxing multiple local organizations (ranging from municipal to state) simultaneously, the aggregate effect created operational disruptions to force projection activities, but no organization was willing to declare it was being attacked, regardless of the perceived antagonist. In any case, the local emergency responders and private entities are likely to be the first to recognize malicious cyber activity if they are targeted; as such, they need the ability to immediately send situational updates to cyber response resources.
   b. When the need for outside assistance becomes obvious, organizations are unsure what support to ask for because they are unsure of the resources that are available. For example, specialty software breaches, such as maritime software packages, require a different skill set than a

Windows breach does. When requesting assistance, municipalities and critical infrastructure sector owners must provide details on what was breached, and they need to know if there are any federal assets available that are trained to assist with the technical challenges of the particular breach.

c. According to Directive-Type Memorandum 17-007, the procedures for reimbursing the DoD for DSCIR are found in DoD 7000.14-R, volume 11A, chapter 3.[26] There are worksheets for determining the personnel costs, yet most still use language and costs associated with physical events and DSCA. The mechanisms and costs associated with requests for DSCA are well established, but the same is not true for DSCIR.

3. **Whether DSCA or DSCIR is the appropriate mechanism for receiving support in the event of a cyber incident that is beyond the ability of local resources to handle, each municipality needs a clear chain of requests, which could include federal or military resources.**

a. During the workshops, execution events, and postevent discussions, it became clear that there was a semantic divide between local-level emergency responders and federal resource providers. DSCA and DSCIR are established processes, but they are not designed to facilitate municipal resource requests. Even requests made through the state government can be difficult to navigate. One federal representative from an organization responsible for coordinating DSCIR requests opined during a workshop that the discussion about DSCIR was irrelevant for JV because municipalities are not part of the process.

b. If DSCIR is indeed inappropriate for municipalities' requests for support, then there should be an alternative avenue for requesting response actions in a controlled manner. JV has shown that national-level interests can be disrupted via local municipality and private company cyber compromises and exploitation.

4. **The mechanisms and request chain for the military to request support from their surrounding community ("reverse DSCIR") need to be explored.**

a. In our force projection scenario, the critical infrastructure disruptions took place within the civilian critical infrastructure between the fort and the port. The communication between the deploying forces and the communities they passed through, which was very limited, focused primarily on law enforcement for traffic management purposes.

b. Though the findings above discuss DSCIR, there may be instances that require the military to request assistance from civilian agencies to resolve technical challenges. Though there are some critical infrastructure facilities located on military posts, installations rely on external forces for the bulk of their critical infrastructure needs.

c. United States Northern Command (USNORTHCOM) and U.S. Army North should explore the possibility of the military requesting civilian assistance with critical infrastructure disruptions that take place outside of an installation but affect military operations within an installation or during movement in the case of force projection.

[26] Work, *Interim Policy and Guidance.*

6.5. Support the Development of an Adaptable and Repeatable Framework

As codified in each JV iteration's research objectives, the prevailing intent has been to develop a JV framework that would allow for this work to be duplicated and scaled. The ACI is a small think tank, and the teams that have developed and planned each JV have been composed of as little as two and as many as six ACI personnel. Though each exercise iteration of the JV research project is comprehensive and provides useful findings, the resource demands and 12- to 24-month planning cycle limit the number of events. Therefore, being responsible for planning and developing these exercises ad infinitum is not sustainable, even with corporate partners supplying additional manpower and resources. The rapid duplication and scaling of JV require a combination of automation and localization that empowers municipalities to plan and execute their own JV-like exercises.

6.5.1. Findings

1. **Every municipality is different, so it is difficult to develop a "one size fits all" framework.**
    a. Though New York City (NYC) and Houston are first and fourth in population size within the United States, respectively, Savannah and Charleston are far smaller, ranking at 182 and 200, respectively.[27] However, Savannah and Charleston are among the port cities through which Army assets deploy overseas and, as such, are strategically important for scenarios requiring force projection from the East Coast. The five locations that participated in the half-day mini-JV exercises support the full spectrum of military service branches, except the United States Space Force.
    b. Within these municipalities are different commercial critical infrastructure organizations with varying relationships with respective their local governments. For example, the ports that the ACI has explored run the gamut from state-owned to partially state-owned to private enterprise. Rigid expectations for local relationships and governance structures would make scaling JV to fit municipalities' needs and circumstances more difficult.
    c. Additionally, because the JV approach is bottom-up, determining municipalities' research and training objectives requires input from the municipality and its associated critical infrastructure organizations. For example, had Charleston and Savannah conducted the same scenario as NYC did in JV 1.0, the exercises would not have fit the cities' needs and circumstances and would not have helped them prepare for a realistic cyberattack scenario in the region.
    d. The DHS Cybersecurity & Infrastructure Security Agency (CISA) also recognized this challenge and developed the CISA Tabletop Exercise Package.[28] The package provides templates for documents required to conduct exercises as well as handbooks to conduct them based on affiliations, such as emergency services and government facilities.
2. **The Law and Policy TTX is an integral part of the framework requirements due to the challenge of translating national-level laws and policies at the local level and differences in laws and policies across states and localities.**
    a. JV 3.0 was the first exercise that spanned two different states, and there were significant differences in the governance structures between the states and the municipalities within those states. Additionally, there are multiple municipalities in both greater metropolitan areas that can play a role in responding to or remediating the effects of malicious cyber aggression.

[27] City and Town Population Totals: 2010–2019," United States Census Bureau (website), last updated May 7, 2020, https://www.census.gov/data/tables/time-series/demo/popest/2010s-total-cities-and-towns.html.

[28] "CISA Tabletop Exercise Package," Cybersecurity & Infrastructure Security Agency (website), n.d., https://www.cisa.gov/publication/cisa-tabletop-exercise-package.

   b. Each organization and participant may be at a different level of cyber maturity and understanding. The Law and Policy TTX was an opportunity to ensure that everyone had a baseline of information on the local area's governance structure, state agencies that address cyber issues and their processes, as well as what should be included in any organizational cyber response plan.
   c. Additionally, the JV 3.0 Law and Policy TTX focused on the procedures for DSCA and DSCIR from a federal perspective. Although DSCA procedures and options are mature and have been exercised by states during natural disasters, DSCIR procedures had not yet been exercised at the time of the Law and Policy TTX in February 2020.

3. **Municipalities do not have the dedicated staff to develop these events internally and will need low- to no-cost assistance to do so.**
   a. Although municipalities are experiencing more and more direct malicious cyber aggression, such as the recent cyberattacks in Texas, Atlanta, and Baltimore, most resources are held at the state level.[29] Discovering cyber incidents is challenging, with 53 percent of successful cyberattacks going undetected until organizations are notified by an outside party. In addition, it takes an average of 197 days to identify breaches and an average of 69 days to contain them.[30]
   b. As of July 31, 2019, there were 19,502 incorporated cities, towns, and villages in the United States, of which 3,092 had a population of 10,000 or more.[31] In 4 years, the ACI has done full JV exercises in four of those places. DHS CISA also conducts critical infrastructure TTXs annually, reaching more locations than the ACI. DHS, CISA, and the ACI are low-to-medium cost options, with the main constraint being availability.
   c. Based on each of the JV iterations as well as feedback from the JV 2.5 workshops, it was evident that state entities had a better understanding of how to plan and execute cyber exercises. When counties or cities seek to conduct an exercise, they place the responsibility of planning them on their IT departments, which tend to be very small. Even if municipalities do use other departments, such as emergency services, they are usually very small, and they may not be familiar with cyber exercise planning.

6.6. Recommendations

Based on the insights and findings from the JV 3.0 exercise, the following recommendations address ways in which organizations could improve cyber resiliency. Although the recommendations include proposed lead organizations, they are only recommendations and do not take into consideration potentially conflicting missions and resources.

6.6.1. Municipalities should consider adopting new internal incident command structures that enable the formation of tailored whole-of-community efforts consisting of synchronized communication, information sharing, and resource allocation during cyber and emergency incident response.

[29] Kate Fazzini, "Alarm in Texas as 23 Towns Hit by 'Coordinated' Ransomware Attack," CNBC, updated August 20, 2019, https://www.cnbc.com/2019/08/19/alarm-in-texas-as-23-towns-hit-by-coordinated-ransomware-attack.html; Stephen Deere, "Feds: Iranians Led Cyberattack against Atlanta, Other U.S. Entities," *Atlanta Journal-Constitution*, November 29, 2018, https://www.ajc.com/news/local-govt--politics/feds-iranians-led-cyberattack-against-atlanta-other-entities/xrLAyAwDroBvVGhp9bODyO/; and Emily Sullivan, "Ransomware Cyberattacks Knock Baltimore's City Services Offline," National Public Radio, May 21, 2019, https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline.

[30] "Cost of a Data Breach Report 2020," IBM (website), n.d., https://www.ibm.com/security/data-breach.

[31] Erin Duffin, "Number of Cities, Towns and Villages (Incorporated Places) in the United States in 2019, by Population Size," Statista (website), June 2, 2020, https://www.statista.com/statistics/241695/number-of-us-cities-towns-villages-by-population-size/.

In conjunction with public and private sector partners, municipalities should explore the adoption of new, agile command structures for cyber incident response that are uniquely adaptable to local community needs. Events like JV can help municipalities identify existing and new pathways for adopting or adapting these structures to best fit their environments. The International Society of Automation Global Cybersecurity Alliance's cyber incident response structure currently in development is just one example of such newly emerging approaches that introduce various integrated roles and a synchronized command structure.[32] Although it focuses primarily on industrial control systems, this concept proposes an adaptable cyber incident command configuration that offers a model for further exploration. Accordingly, municipalities should not only explore such emerging efforts, but also actively seek to inform their creation. Doing so will help ensure these new frameworks possess a necessary agility that lends itself to effectively supporting local community resilience during cascading cyber incidents.

6.6.2. Establish a mentorship program between municipalities that encourages information sharing and joint cybersecurity exercises. The partnership program provides a safe learning environment in which local organizations can further develop their working relationships.

There is a broad spectrum of cybersecurity organization and maturity across the United States. DHS CISA is in the best position to create a mentorship program that could pair similar cities, counties, school districts, and military posts/camps/stations based on population, industry, etc., and their assessed cybersecurity posture. This partnership program would provide a safe venue in which smaller organizations and governments could learn best practices for cybersecurity, cyber incident response, and information sharing and coordination. Furthermore, the program would facilitate the development of cyber resilience from the bottom up and provide an ideal venue in which state and federal entities could evaluate the effectiveness of policies and procedures.

6.6.3. Federal, state, and local leaders must recognize cybersecurity and cyber incident response as a key responsibility and allocate resources to personnel, training, and education shortfalls accordingly.

The participants who had a higher degree of confidence and competence in cybersecurity, whether it was from prior real-world experience or training, rapidly oriented themselves to the cyber-focused scenario injects; quickly became attuned to their potential impacts; and began the decision-making process in support of incident response, mitigation, and remediation. Given the rapid evolution of the cyber domain, which includes the complexities of operational technology (OT) / IT integration, there is a critical need for including cybersecurity experts as part of both IT departments and foundational security programs for every sector and level of government. Leaders must understand that IT and information security are related but distinct disciplines, and then resource organizational staffing and responsibilities accordingly. Despite the shortage of cybersecurity professionals, organizations should continue to formalize and refine response plans in addition to resourcing training programs and conducting exercises to help close the gap.[33] Furthermore, entities such as DHS and state-level cyber responders can assist by providing standardized, accessible, and relevant tools for city governments that may not have the time, capability, or resources to provide adequate cybersecurity. Where plans rely on requests for additional support, the thresholds for requesting support should be identified in advance and the procedures for requesting support rehearsed regularly. Only through experience, training, and preparation can we successfully respond to current threats while building future generations of responders.

[32] "Incident Command System for Industrial Control Systems," S4xEvents (website), n.d., https://s4xevents.com/ics4ics/.

[33] Steve Durbin, "10 Benefits of Running Cybersecurity Exercises," Dark Reading, December 28, 2020, https://www.darkreading.com/operations/10-benefits-of-running-cybersecurity-exercises/a/d-id/1339709.

6.6.4 State cyber and emergency incident response entities, such as the SC Critical Infrastructure Cybersecurity (SC CIC) program within SLED and the Georgia Emergency Management and Homeland Security Agency (GEMA), should work to establish standing, mutually supportive cyber resource support agreements that utiltze the Emergency Management Assistance Compact framework and Mission Ready Packages to build regionally focused cyber incident response and support plans for responding to a cascading cyber incident.[34]

JV 3.0 highlighted the potential value of creating cyber-focused memoranda of understanding (MOUs) within states and Emergency Management Assistance Compacts between neighboring states that can be utilized during significant cyber incidents, thereby providing critical cyber personnel, resources, and capabilities that already reside in the affected region. For example, SC CIC maintains MOUs with close to 100 organizations throughout the state that allow the 125th Cyber Protection Battalion, South Carolina (SC) National Guard—a member of SC CIC—to conduct on-site incident response with the consent of the governor. For regional, cyber-focused Emergency Management Assistance Compacts, the design must remain a state-led effort to ensure the proper tailoring of support packages that can adequately account for the unique characteristics of each state. These support packages should be formalized to include standing, tailored, regional cyber response Mission Ready Packages that can increase the speed, agility, and capability of support while ensuring the transparency of requirements and cost.[35] The DoD and DHS should help foster and support these efforts: The DoD should do so through defense coordinating elements (DCEs), and DHS should do so through the Federal Emergency Management Agency and DHS CISA. Ensuring federal stakeholder presence can support additional meaningful facilitation and dialogue regarding resource sharing, gaps, and concerns. Additionally, having federal stakeholder support will also help bridge the gap between federal, state, and municipal cyber incident response efforts.

6.6.5. Federal and state entities should execute annual law and policy TTXs that extend to municipalities and private industry. These events provide a venue in which leaders and responders can identify gaps in authorities, rehearse resource requests, and identify potential thresholds. In particular, State and National Guard response authorities and mechanisms differ by state and locality, and these will continue to evolve as cyberspace is better understood. As such, the law and policy TTXs will be critical for understanding the roles and responsibilities associated with utilizing National Guard resources.

The law and policy TTX ensures all participants have a common understanding of the legal and political frameworks in which they are operating as well as an opportunity to review internal organizational policies and procedures prior to the exercise. Though it has been included in each iteration of JV to ensure participants have a baseline of knowledge, leaders and responders at all levels should adopt the event to improve expertise on response authorities and requesting resources. Furthermore, these types of TTXs are important for exploring the DSCIR process, which remains a relatively novel process that is not regularly executed nor exercised. It is recommended that these exercises be executed in conjunction with training on applicable laws in the area, existing policy documents, and historical cyber responses.

[34] "Emergency Management Assistance Compact," Federal Emergency Management Agency (website), n.d., https://www.fema.gov/pdf/emergency/nrf/EMACoverviewForNRF.pdf.

[35] National Emergency Management Association, "Mission Ready Packages," Emergency Management Assistance Compact (website), n.d., https://www.emacweb.org/index.php/mission-ready-packages.

6.6.6. Federal and state agencies should design and establish a data repository for resources and data related to cyber incidents, tailored responses, impacts, and exercises to facilitate the sharing of policies, procedures, best practices, data, and emerging issues. The repository should be open for municipalities and private entities to deposit and utilize resources to increase the resilience of their associated critical infrastructure.

Events like JV exercises generate a lot of information, including policy information, best practices, and raw data. If available to verified users at the city, state, and federal level, access to and analysis of this data would prove useful in assessing cybersecurity programs and resource allocation. State and federal agencies would facilitate critical infrastructure research and resiliency by establishing a single repository for securely storing this data. Properly anonymized, this data would allow agencies to study trends in their areas of responsibility. An example of this initiative is SC CIC's Cyber Posture Review, an assessment of critical infrastructure entities' cybersecurity posture. The Cyber Posture Review collects and analyzes anonymized data to evaluate the overall cyber posture of the state. Cities and municipalities would benefit from this single certified repository because it would contain reliable resources and tools for assisting in the assessment, development, and improvement of the organizations' cyber resilience.

6.6.7. DHS, in concert with the DoD, should examine and potentially expand the United States Coast Guard Cyber Command's (CGCYBER's) authorizations, resources, and mission set to include initial cyber incident response support for strategic ports and port cities.

With CGCYBER focused on defending its portion of the DoD Information Network, protecting the maritime transportation sector, and further enabling cyber operations,[36] the DoD should examine provisioning additional resources to further develop the relationship and grow the number of trained, resourced, and readily available CGCYBER Cyber Protection Teams that can provide incident response support to strategic ports and local municipalities. USCG maintains several unique authorities, such as Title 14 (Coast Guard), Title 40 (law enforcement under DHS), Title 10 (warfighting under the DoD), Title 50 (intelligence), and Title 33 ("captain of the port") authorities that enable speed, agility, and flexibility when coordinating not only a whole-of-government response, but also a whole-of-community approach through incident diagnoses, information sharing, and remediation efforts.[37] USCG is uniquely positioned to help spearhead immediate response actions at strategic port locations in support of domestic critical infrastructure resilience and Army force projection operations. USCG cyber capabilities remain fully interoperable with both the DoD and DHS in support of homeland defense efforts;[38] indeed, a standing cybersecurity and cyberspace operations memorandum of agreement already exists pursuant to Title 10 and Title 6 authorities.[39] Additionally, as an active member of the Maritime Transportation System Information Sharing and Analysis Center, USCG maintains robust local and industry partnerships that will further facilitate a whole-of-community response.[40] Accordingly, DHS, as the lead agency, should work with other supporting agencies, such as the DoD, in examining how allocating additional resources (funding, training,

[36] Kimberly Underwood, "The Coast Guard Jumps into the Cyber Sea," SIGNAL, February 1, 2019, https://www.afcea.org/content/coast-guard-jumps-cyber-sea.

[37] Underwood, "The Coast Guard Jumps."

[38] J. R. Wilson, "CGCYBER and Coast Guard Cybersecurity." Defense Media Network, March 14, 2018, https://www.defensemedianetwork.com/stories/coast-guard-cybersecurity/.

[39] Department of Defense (DoD) and Department of Homeland Security, *Memorandum of Agreement between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations* (Washington, DC: DoD and Department of Homeland Security, 2017).

[40] "MTS-ISAC Services," Maritime Transportation System ISAC (website), n.d., https://www.mtsisac.org/services, accessed January 11, 2021.

and authorities), personnel authorizations, and capabilities can help expand CGCYBER's mission scope to include cyber incident response and resilience efforts at strategic ports of embarkation.

6.6.8. Through the respective garrisons, U.S. Army Installation Management Command should work to develop, incorporate, resource, and exercise a tailored cyber incident response annex within its emergency incident response plans for force projection and deployment operations.

The Army has introduced a strategic framework that recognizes the ever-increasing likelihood that adversaries will target installations through cyber-enabled threat vectors.[41] As this strategy continues to take shape, garrisons should synchronize and integrate resources, capabilities, and response protocols with municipal, state, federal, and private sector partners as appropriate. Garrisons should look for additional opportunities to embed, exchange, and cross-train personnel along with their municipal and private sector partners to build partnerships, shared understanding, and a common operating picture for responding to both physical and cyber incidents. It is also important that installations overseen by U.S. Army Installation Management Command have educated, knowledgeable, and trained resources who can recognize cyber activities that could be deliberate or system failures that impact day-to-day operations as well as force projection activities.

6.6.9. DoD planners must utilize integrated campaigning at multiple echelons (city, county, and state) to understand adversary actions against interorganizational partners and better inform campaign plan assumptions.

JV 3.0 provided a narrow glimpse into the impact that cyber incidents targeted at the city and county level can have national implications, particularly with respect to force projection. One can no longer assume freedom of movement in the current operating environment, and stakeholders will only gain a better appreciation of the impacts by studying commercial and interorganizational partners' responses to and resilience against cyber incidents. The municipality focus of JV provides a structure that allows planners to understand how adversary actions impact these partners and subsequently inform the design and construction of campaign plans.

6.6.10. In conjunction with academic and government partners, the ACI should develop and implement automated tools that will allow novice planners to rapidly design and quickly execute JV-like events.

One of the critical goals of the JV series is to develop a repeatable and adaptable framework that reduces the time and difficulty involved with planning a cyber-incident response exercise. The ACI is producing static and generic guides, but these guides are a temporary solution because they do not provide a dynamic system that will tailor programs to a particular city or objective. The ACI is developing a suite of tools designed to automate the JV documents. Expected to achieve initial operating capability by March 30, 2021, the automated toolset includes a planner application that allows municipal and organizational planners to input, at a minimum, lists of their sector/subsector critical infrastructure, the length of their exercises, their exercise start dates, their difficulty levels (by sector), their locations, and the organizations that will be participating. The application will return a Master Scenario Event List (MSEL) for review and approval to the planner. Once finalized, the system will generate an Exercise Planning Guide, Player Handbook, and Data Collector Handbook for the planner to download as well as a file that can be imported into the Norwich University Applied Research Institute (NUARI) DECIDE® platform with the MSEL for conducting a TTX.

[41] *U.S. Army, Army Installations Strategy* (Washington, DC: U.S. Army, December 2020), 1–22.

7. CONCLUSION

Cybersecurity is critically important for the United States now, and it will continue to be so in the future. Increasing threats from criminal and nation-state actors reinforce the growing need for collaboration, communication, and a whole-of-community approach to defending and responding to cyber incidents. Effective defense does not come without a cost; it requires significant planning, exercise, and leadership—leadership at all levels, but, particularly, leadership inherent to organizations with large reach and impact. The new presidential administration's emphasis on cybersecurity, including recent appointments to the National Security Council and ongoing enhanced collaboration between DHS and the FBI as they work toward joint, proactive operations, indicates leadership at the highest levels are taking positive steps toward this effective defense.

Despite these positive steps toward cyber defense, gaps still exist in coordinating and resourcing municipality and private critical infrastructure resilience. The ACI's JV series helps municipalities, counties, and critical infrastructure stakeholders improve their resilience through exercising their cyber incident response plans and improving their communication networks. The ACI has now completed three iterations of JV and placed significant emphasis on preparation and planning. The JV series provides an essential training and exposure venue to many small and medium-sized government agencies while enhancing the Nation's ability to respond to a cyber crisis.

Findings from JV 3.0 highlight the value of the event to the U.S. Army in planning force projection and helping cities and counties improve their cyber incident response and information sharing. This research reinforces critical concepts of preparation that impact force projection, including whole-of-community participation, interdependency comprehension and communication, and the perpetual merit of exercises with multiple critical infrastructure elements. Moreover, this most recent iteration of JV demonstrated that any distinction in municipality size is void when it comes to the potential for national and strategic implications stemming from a cascading cyber incident. Though JV 3.0 provided new insights into cyber incident response, it also identified several findings similar to those of previous iterations:

- There is no clear threshold for the declaration of a potential critical cyber incident;
- Traditional incident response continues to be more mature than cyber incident response; and
- Cross-sector communication continues to be a challenge.

The consistent theme of these findings throughout the JV series not only necessitates the continuation of multisector events, but also the enhancement and evolution of the program. Not only do the recommendations of the current and past iterations of the JV program provide an immediate way forward, but they also serve as a strong foundation for future cyber exercises that are likely to occur on an even more expansive scale. The *Cyberspace Solarium Commission Final Report* highlighted the importance of cyber exercises and recommended expanding coordinated cyber exercises and establishing a biennial national cyber TTX.[42] These goals were furthered when they were addressed in the National Defense Authorization Act for Fiscal Year 2021, which calls for a biennial exercise that would involve federal, state, private sector, and international stakeholders.[43] The execution of JV has demonstrated the necessity of including local and private industry partners in these exercises

[42] U.S. Cyberspace Solarium Commission, *Cyberspace Solarium Commission Final Report*.

[43] National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283 (2021).

and provided an example for how to accomplish coordination all levels. The continued evolution and expansion of the program is a critical element in our national effort to establish and maintain a robust cyber defense and response capability founded on partnership, collaboration, and communication. To be prepared and organized in advance of the next big event, critical infrastructure stakeholders, including the U.S. Army and the DoD, must continue to evolve. Practice is a critical and essential component of that evolution, and JV is a proven and effective foundation for that practice.

APPENDIX A – ACRONYMS

Acronym	Definition
3ID	3rd Infantry Division
ACI	Army Cyber Institute
AHA	All Hazards Analysis
ARCYBER	United States Army Cyber Command
ARNORTH	U.S. Army North
BDE	Brigade
CAPEC-ID	Common Attack Pattern Enumeration and Classification identifier
CGCYBER	United States Coast Guard Cyber Command
CIRI	Critical Infrastructure Resilience Institute
CISA	Cybersecurity & Infrastructure Security Agency
CJCS	Chairman of the Joint Chiefs of Staff
CMAW	Cyber Mutual Assistance Workshop
COVID-19	Coronavirus disease 2019
D1	Disruption 1
D2	Disruption 2
D3	Disruption 3
DC	District of Columbia
DCE	Defense coordinating element
DCI	Defense critical infrastructure
DCO	Defense coordinating officer
DECIDE®	Distributed Environment for Critical Infrastructure Decision-making Exercise
DHS	Department of Homeland Security
DIB	Defense industrial base
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOE	Department of Energy
DSCA	Defense Support to Civil Authorities
DSCIR	Defense Support to Cyber Incident Response
DV	Distinguished visitor
ELD	Electronic logging device
EM	Emergency management
FBI	Federal Bureau of Investigation
FD	Fire department
FEMA	Federal Emergency Management Agency
GA	Georgia
GCC	Georgia Cyber Center
GEMA	GA Emergency Management and Homeland Security Agency
GIS	Geographic information system

Acronym	Definition
GNSS	Global Navigation Satellite System
GOS	Gate operating system
GPS	Global Positioning System
HIFLD	Homeland Infrastructure Foundation-Level Data
ICODES	Integrated Computerized Deployment System
ICS	Industrial control system
INL	Idaho National Laboratory
IPM	Initial planning meeting
IT	Information technology
JHU APL	Johns Hopkins University Applied Physics Laboratory
JV	Jack Voltaic
LEC	Local exchange carrier
LFX	Live-fire exercise
LH	Line haul
MEF	Mission Essential Function
MITM	Man in the middle
MOU	Memorandum of understanding
MPH	Miles per hour
MPM	Midplanning meeting
MSEL	Master Scenario Event List
MTS	Maritime Transportation System
NATO	North Atlantic Treaty Organization
NG	National Guard
NUARI	Norwich University Applied Research Institutes
NYC	New York City
OPT	Operational Planning Team
OT	Operational technology
PD	Police department
PDT	Port Disruptions Tool
PLC	Programmable logic controller
POA&M	Plan of action and milestones
RDD	Required Delivery Date
RDP	Remote Desktop Protocol
ROC	Rehearsal of Concept
SATCOLT	Satellite on light truck
SC	South Carolina
SCADA	Supervisory control and data acquisition
SC CIC	SC Critical Infrastructure Cybersecurity
SDDC	Military Surface Deployment and Distribution Command

Acronym	Definition
SLED	SC Law Enforcement Division
SPOD	Seaport of debarkation
SPOE	Seaport of embarkation
SRNL	Savannah River National Laboratory
STC	Savannah Technical College
TOS	Terminal operating system
TRANS	Transportation
TTX	Tabletop exercise
TWIC	Transportation Worker Identification Credential
UAV	Unmanned aerial vehicle
UIUC	University of Illinois at Urbana-Champaign
USA	U.S. Army
USAG	U.S. Army Garrison
USB	Universal Serial Bus
USCG	United States Coast Guard
USGS	United States Geological Survey
USMC	United States Marine Corps
USNORTHCOM	United States Northern Command
USTRANSCOM	United States Transportation Command
WI	Wisconsin

Table 6: Acronyms

APPENDIX B – PARTNERS

B.1. Partners

The ACI works with partners with mutual interests that aim to resolve similar issues. Preventing future cyber-related crises can become a reality through establishing public-private, academic, and industry relationships with relevant experts. Furthermore, JV 3.0 and Jack Pandemus would not have been possible without these partners.

The following sections elaborate on the ACI's JV partners and their respective roles in JV 3.0.

B.2. Core Partners

B.2.1. City of Charleston

For the City of Charleston, participating in JV 3.0 was a positive experience, and the takeaways were extremely valuable. The presented scenarios allowed for the opportunity to examine current procedures within the city's operations, assess potential shortcomings, and identify possible communication links that could be established both within the city and with external, regional organizations. Better communication with these agencies would provide for enhanced situational awareness of events in the region and, potentially, earlier detection of a coordinated event involving multiple targets. The exercise also allowed for a detailed exploration of the procedures that would be utilized to notify SLED and the SC Critical Infrastructure Cybersecurity program of a potential or active cyber event. Charleston would use these procedures to request assistance from state agencies and coordinate the notification of federal agencies. Perhaps the most valuable benefit of the exercise was the opportunity to create working relationships with other security professionals. The face-to-face interactions during the planning meetings provided participants with the chance to introduce themselves to colleagues with whom they did not normally interact. As a direct result of the exercise, Charleston cybersecurity staff and other regional professionals created a working group to exchange ideas and information about challenges they face in their respective environments.

B.2.2. City of Savannah

The City of Savannah, GA, was involved early in the planning process. Led by the City of Savannah emergency management director, the IT, emergency preparedness, fire, and water resources departments became significantly involved in the planning. Savannah's emergency manager and IT department served as the city's points of contact for the exercise, introducing ACI to critical stakeholders in the area. In addition to supporting and attending the ACI meetings, Savannah held its own internal meetings to discuss and determine participation. The city also finalized its Cyber Incident Annex as part of its preparation. Savannah had 18 personnel from multiple agencies participate in the Rehearsal of Concept (ROC) Drills and exercise. The local police department participated in the ROC Drills, but it could not make the final exercise because its participation was preempted by a real-world incident.

Savannah considered the JV exercise to be a success for the city. Its well-established and well-developed relationships with local stakeholders—mainly, other government entities—and effective internal communications proved to be advantageous during the exercise.

The exercise also provided Savannah with opportunities to examine its protocol regarding cybersecurity, including the following recommendations for the future:

- Savannah needs to identify and engage additional community partners (e.g., private sector organizations and utilities) well before an incident occurs.
- Personnel staffing and role assignment were issues because the same people potentially fill multiple functions in incident response.
- Savannah identified areas where the city's IT department needs to be engaged prior to an incident. These areas relate to department-specific needs, such as:
  - Researching how the fire department's mobile data terminals might be impacted by a complete communications blackout; and
  - Examining how a complete communications blackout might affect the city's water and sewer resources' networks, including SCADA and other systems.
- Savannah acknowledged the need to conduct follow-on exercises to address gaps and assemble a whole-of-community response.

Savannah's IT department identified the following as areas for improvement:

- Check agreements and contracts for the parameters of cyber incident response support.
- Ensure continuity of operations for the city data center during a long-term power outage.
- Strengthen city policies regarding the doxing of employees.
- Examine how attacks would affect the city as a whole and what external partners would need to be notified. For example, Savannah's IT department believes it must address potential cross-system issues between the city network and isolated networks, such as SCADA and traffic management systems.

B.2.3. FTI Consulting

FTI Consulting is a global business advisory firm dedicated to helping organizations manage change; mitigate risk; and resolve financial, legal, operational, political and regulatory, and reputational and transactional disputes. The ACI partnered with FTI Consulting's Cybersecurity team, which takes an intelligence-led, expert driven, strategic approach to global cybersecurity challenges affecting organizations through a trusted core of comprehensive offerings. This enables clients of any size to address their most critical needs and integrate new solutions atop or alongside preexisting policies and programs to address cyber threats.

FTI Cybersecurity was introduced to the ACI and JV 3.0 through existing relationships with FTI Cybersecurity personnel and members of the DoD. When the topic of JV 3.0 arose, FTI Cybersecurity welcomed the opportunity to support the ACI in the implementation of this innovative research project, confident that it had a significant ability to leverage its cybersecurity expertise, global representation, and professional consultancy to enhance research exercise development and implementation.

Representing the private sector and the cybersecurity industry, FTI Cybersecurity partnered with the ACI to cosponsor JV 3.0. More than a dozen FTI Consulting team members, including senior executives and segment subject matter experts, participated in JV 3.0.

Private sector collaboration on this venture served to enhance the ACI's capabilities, ensuring successful implementation of the TTX and the development of strategic partnerships in defense of the Nation's critical infrastructure.

Before the pandemic and once pandemic measures had been implemented, FTI Consulting worked with the ACI to complete several critical elements of the project, including but not limited to:

- Planning for and recruiting participants and recommending additional regional and local partners from SC and GA for the exercise.
- Collaborating on and shaping the key concepts and planning considerations for the exercise, including:
  - Setting the exercise foundation by reviewing guidance, training exercise plans, and other sources;
  - Selecting participants for the Planning Team and developing a plan of action and milestones;
  - Developing exercise-specific objectives and identifying core capabilities; and
  - Contributing to the exercise manual and the facilitator/controller handbook.
- Drafting the exercise scenario and significantly contributing to event and inject development.
- Providing input for the development of a research proposal, executive information sheet, Army objective information sheet, JV 3.0 technical report for senior leadership, JV 3.0 technical academic report with lessons learned, and After Action Review summary.
- Engaging in a collaborative review of jurisdiction-specific threats and hazards; areas for improvement; external requirements, such as state or national preparedness reports; homeland security policy; and accreditation standards, regulations, and legislative requirements.
- Planning and supporting the Law/Policy TTX, including leading the discussion and presentation on cyber insurance.
- Supporting the execution of Jack Pandemus, a distributed functional exercise in support of JV 3.0.
- Supporting the planning of the LFX, though it ultimately did not occur because of complications arising from COVID-19.
- Developing and executing a communications outreach plan, including coordinating with Cyberscoop for an interview.
- Incrementally increasing staffing as the exercise requirements increased. FTI Consulting continually added support as additional requirements arose, including the provision of moderator support for Jack Pandemus and JV 3.0.
- Providing video development for the Executive Out-Brief.

Also, prior to the pandemic, FTI Consulting sponsored Distinguished Visitor (DV) Day, which would have included keynote speakers, staffing support, and food services at both venues. Once the JV event switched to virtual execution, DV Day became the Executive Out-Brief, for which FTI Consulting conducted the scenario presentation and supported the development of briefing materials.

B.2.4. NUARI/DECIDE®

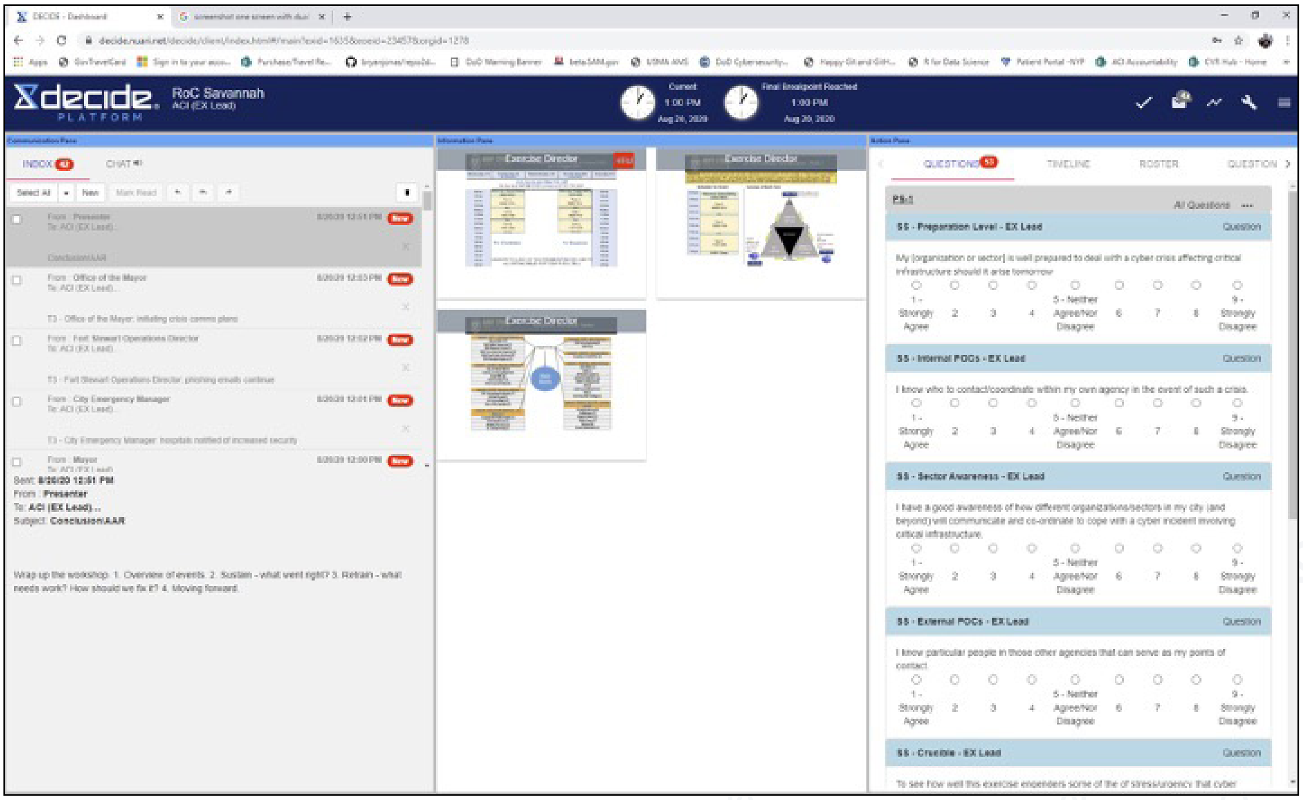
NUARI partnered with the ACI for JV 3.0. NUARI is a 501(c)(3) non-profit that serves the national public interest through the interdisciplinary study of critical national security issues that is partially funded by DHS and the DoD and federally chartered under the sponsorship of Senator Patrick Leahy. NUARI provides cyber exercises; secure network monitoring; and custom consulting, research, and education through many avenues, including its DECIDE® exercises.

Initially conceived and started independently by NUARI and developed with funding from DHS, DECIDE®—an exercise platform—simulates cyberattacks and natural disasters for organizations and their partners to stress and test incident and emergency response plans, resulting in after-action reports that lead to improved strategic communication, compliance, risk, and overall resilience. The DECIDE® platform has been a trusted cybersecurity LFX solution for more than 10 years.

How DECIDE® Works

The DECIDE® platform powers LFX-based scenarios to help decision-makers in critical infrastructure sectors, private industry, and government to exercise their abilities to effectively prepare for and respond to cyber and emergency response incidents in a fully distributed environment. DECIDE® exercises allow users in a variety of geographic locations to conduct collaborative, realistic, fully immersive, scenario-based exercises where the consequences of each action feeds back into the exercise. The exercises are designed to help players understand the systemic ramifications of their actions and improve communication during potential high-stress threat events. DECIDE® also supports and facilitates discussion-based TTXs for much quicker and easier capture, review, and analysis of the exercise for immediate use upon completion.

When participants log in, they have access to three panes: the Communication pane on the left, the Information pane in the middle, and the Actions/Questions pane on the right. NUARI's development team loads the exercise into the tool from an MSEL and roster. At the top, the day and time is displayed and can be advanced by minutes, hours, days, weeks, or years. This allows the exercise to simulate a multiday event and document responses, actions, and notes from participants at certain times. When an exercise is complete, the tool will have captured the relevant information associated with the exercise. The tool then organizes the information chronologically for easy analysis and evaluation of the results.



RoC Savannah
ACI (EX Lead)

From : Presenter
To: ACI (EX Lead)...
8/20/20 12:51 PM New
Conclusion/AAR

From : Office of the Mayor
To: ACI (EX Lead)...
8/20/20 12:03 PM New
T3 - Office of the Mayor: initiating crisis comms plans

From : Fort Stewart Operations Director
To: ACI (EX Lead)
8/20/20 12:02 PM New
T3 - Fort Stewart Operations Director: phishing emails continue

From : City Emergency Manager
To: ACI (EX Lead)...
8/20/20 12:01 PM New
T3 - City Emergency Manager: hospitals notified of increased security

From : Mayor
To: ACI (EX Lead)
8/20/20 12:00 PM New

Sent: **8/20/20 12:51 PM**
From : **Presenter**
To: **ACI (EX Lead)...**
Subject: **Conclusion/AAR**

Wrap up the workshop. 1. Overview of events. 2. Sustain - what went right? 3. Retrain - what needs work? How should we fix it? 4. Moving forward.

PS-1 All Questions

SS - Preparation Level - EX Lead Question

My [organization or sector] is well prepared to deal with a cyber crisis affecting critical infrastructure should it arise tomorrow

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Internal POCs - EX Lead Question

I know who to contact/coordinate within my own agency in the event of such a crisis.

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Sector Awareness - EX Lead Question

I have a good awareness of how different organizations/sectors in my city (and beyond) will communicate and co-ordinate to cope with a cyber incident involving critical infrastructure.

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - External POCs - EX Lead Question

I know particular people in those other agencies that can serve as my points of contact

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Crucible - EX Lead Question

To see how well this exercise engenders some of the of stress/urgency that cyber

Figure 16: Once participants logged into DECIDE®, they loaded this three-pane screen to view the Communication (left), Information (middle), and Actions/Questions (right) panes.

The ACI and NUARI initiated the partnership in January 2020. NUARI joined the ACI's first planner workshop in Savannah, GA, 4 days after the first call. DECIDE® provided the platform for a fully distributed, 8-hour exercise for the cities of Savannah and Charleston. NUARI also worked frequently and closely with the entire Planning Team on a weekly basis. It was an enjoyable experience for the NUARI team, and the organization gained valuable insights working with the different exercise planners from the organizations involved.

Due to COVID-19 travel and distancing restrictions, exercise execution with participants in the same space was not feasible. Without DECIDE®, execution of JV 3.0 in 2020 would not have been possible. Because DECIDE® was created to facilitate distributed TTXs and LFXs with participants in a variety of geographic locations, it was a natural transition for the DECIDE® tool to facilitate the execution of the full JV 3.0 exercise from a remote, or distributed, position.

DECIDE® equips organizations, exercise divisions, consulting organizations, the military, and governments with the ability to exercise any type of response plan through a discussion-based TTX or full-scale functional exercise in a remote, or distributed, modality. It captures information that describes objectives set for the exercise and outlines them, allowing for analysis and prescriptive discussion to take place in order to improve resilience. It saves time for the subject matter experts facilitating the exercise and provides timely and meaningful information for the participating organizations. DECIDE® brings actors from across sectors, geographies, and roles together into a distributed environment to facilitate participation in critical infrastructure exercises.

B.3. Major Contributors

B.3.1. Intrepid Networks

Intrepid Networks provides both products for mission- and business-critical operations and custom development services—including the development of unique software applications, embedded firmware design, and low-cost communication hardware—for government agencies. Its flagship solution, Intrepid Response, is a FirstNet-certified and affordable web and mobile situational awareness software platform for day-to-day and emergency operations. Mapping, information sharing, team mobilization, emergency notification, and push-to-talk voice communications are integrated into an easy-to-use and deployable solution, enabling instant team communication, coordination, and collaboration over a common operating picture. Intrepid Response is uniquely designed to support users in the field engaging in day-to-day operations and incident and emergency management, base security, and surveillance operations.

Designated as the JV mobile situational awareness and collaboration software platform, Intrepid Response provides a common operating picture across federal, state, and local government and civilian organizations for coordinated response to cyberattacks.

For JV 3.0, Intrepid Response provided a turn-by-turn common operating picture of events that unfolded as a result of organized cyberattacks in the cities of Charleston and Savannah. The Intrepid Response capability enabled the rapid recognition of seemingly random events as having resulted from a persistent and coordinated cyberattack. This rapid recognition was shown to be instrumental for disparate stakeholders across federal, state, and local agencies to rapidly recognize, launch, and execute a coordinated, collaborative response while maintaining a real-time common operating picture.

B.3.2. FirstNet/AT&T

As described in section 4.5.6, FirstNet, built in partnership with AT&T, is a Nationwide public safety broadband network that delivers interoperability for all first responders across agencies and jurisdictions. A common platform that was designed with and for first responders, FirstNet is addressing the needs resulting from extremely fast-paced technology development coupled with government IT infrastructure limitations in handling the increasing demand for capacity, better coverage, and stronger security.

AT&T was originally going to provide a full suite of FirstNet equipment for the JV 3.0 exercises before the pandemic forced the events to move to a virtual format. AT&T, however, still provided a team of subject matter experts to participate in both planning and execution of the exercises. As a result, the team discovered the disaster response communications needs and limitations of local and state governments and how FirstNet can be applied to strengthen emergency response.

During the exercises, the AT&T team was afforded a unique view into city IT operations from both a cybersecurity and a staffing perspective. It became clear that though the players were willing and able to grasp new ideas and technologies, additional education, training, and network upgrades are needed to enable disaster response communications to benefit from technologies like FirstNet and other wireless technology advancements.

The fifth generation of cellular wireless technology, 5G, has the potential to offer massive connectivity and faster speeds that can transform how public safety and emergency response operate. AT&T is already working with the First Responder Network Authority on the best way to make 5G available to first responders. Other network upgrades that will support 5G include increasing capacity and coverage, adding fiber-optic infrastructure, enhancing the core network to support lower network latency (for a faster overall network), and adding tower equipment that can be upgraded through software.

The JV 3.0 exercises highlighted the vulnerabilities of municipality and other stakeholder IT security systems as well as the heightened threat environment and consequences of hacks and breaches. Network security is particularly crucial for public safety systems like FirstNet. Although 5G will allow for more innovation and efficiency, it will also require enhanced security measures. The network is the engine that keeps agencies and organizations running. For effective emergency response and operations in general, it is crucial for local and state governments to leverage multiple layers of security across applications, devices, networks, and platforms. This redundancy will help reduce the risk of exposure to attacks, whether they occur within or outside the network.

The Internet of Things is a network concept that can vastly improve agency operations by facilitating a rapid growth in the number of connected devices and sensors on everything from borders to buildings. AT&T Control Center, an automated connectivity management platform, can manage and monitor data generated from, and the connectivity of, Internet of Things devices enabled with FirstNet-capable subscriber identification modules over the Nationwide public safety broadband network in near-real time. Control Center for FirstNet is a cloud-based platform that simplifies the deployment and management of connected devices and Internet of Things solutions for public safety entities through diagnostic and automation capabilities, multilayered security, service reliability, and usage monitoring.

JV 3.0 illustrated that reducing the complexity and cost of fighting cybercrime is an imperative, yet daunting, task. Local and state governments should become educated on and invest in resilient and redundant systems so that they may continue operations in the face of disruptive or destructive cyberattacks on their networks. FirstNet can transform the emergency management environment through the priority connectivity needed to protect local communities and support those who protect our homeland.

B.3.3. The Citadel

The Citadel, located in Charleston, SC, offers a classic military college education for young men and women focused on leadership excellence and academic distinction. The Citadel, which is recognized as a National Center for Academic Excellence in Cyber Defense Education by the National Security Agency and DHS, established the Center for Cyber, Intelligence and Security Studies in 2016.

The Citadel hosted a JV 2.5 workshop in Charleston on May 21, 2019. The college worked with the ACI to organize the workshop. In addition, faculty from The Citadel supported the planning efforts, attending the JV 3.0 Initial Planning Meeting in Augusta, GA, on July 9–10, 2019; numerous planning workshops; and the ROC Drill for Charleston on September 8, 2020. Faculty and students from The Citadel participated in the exercise itself, serving as both participants and data collectors.

B.3.4. Savannah Technical College

Savannah Technical College (STC) serves coastal GA by providing quality, market-driven technical education at campuses in Chatham, Effingham, and Liberty counties STC is a proven, reliable source of cybersecurity experts: It has a 99.1-percent job placement rate, with 94.6 percent of its students employed in their respective fields of study, according to a survey conducted in academic year 2019. Under the direction of Lt. Col. Scott C. Scheidt, USA (Retired), the Cybersecurity Workforce Education Center was launched in 2020 as a multidisciplinary cyber defense education center to meet the growing demands of the national cybersecurity workforce shortage and provide training support along with cyber-related advisory services to municipal and industry partners in the area. The Cybersecurity Workforce Education Center offers degrees with the following specializations: computer support specialist, networking specialist, cybersecurity, and cyber forensics technology. In addition, STC has built a cyber range with the help of a federal Perkins grant that will support cyber workforce training.

The ACI and STC began working together in January 2020. STC provided academic advisory support and facilitated face-to-face meetings prior to COVID-19. Also prior to COVID-19, the ACI and other key partners completed a site visit and approved STC as the on-site location of the Savannah JV 3.0 exercise.

When COVID-19 caused a change from face-to-face to virtual execution, STC offered to provide a cadre of data collectors from the Cyber Workforce Education Center. More than 15 students registered to help as data collectors for the Savannah iteration of the exercise. This not only facilitated success for JV 3.0 data collection, but also allowed students to gain valuable knowledge and insight into cyber readiness needs and methods that the students perhaps would not have received otherwise. The data collectors are now knowledgeable advocates for cyber readiness exercise planning and integration. In addition, faculty from STC served as members of the DV Day and Scenario Design and Execution OPTs. In the future, STC will collaborate with the ACI to incorporate the JV experience into training exercises in the coastal GA region.

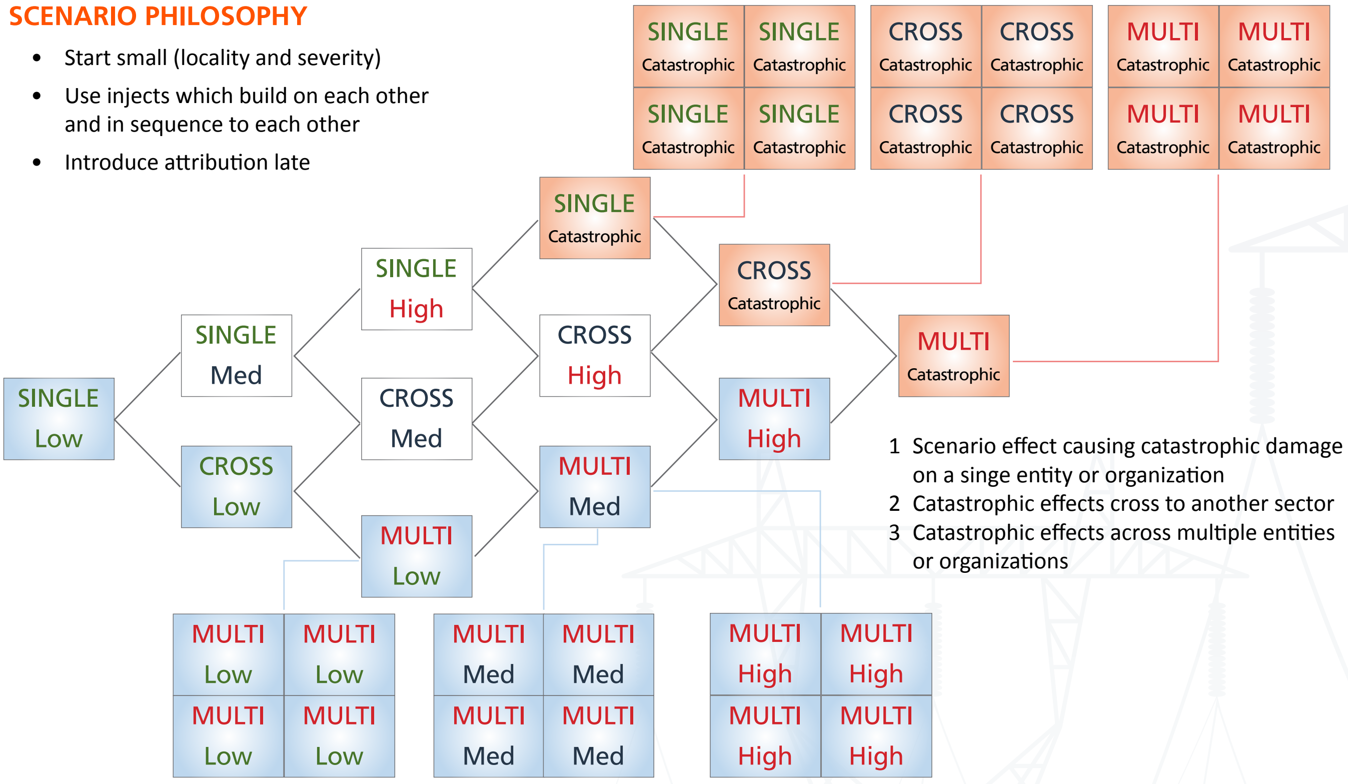
B.3.5. Blank Slate Solution

Blank Slate Solution of Mount Pleasant worked to establish critical connections to local and state government that enabled the ACI to develop and execute JV 2.5 and 3.0. The company collaborated with the ACI on all events to ensure that participants received the greatest understanding of and appreciation for information warfare response and policy. The company also served as a member of the JV 3.0 data collection team. Blank Slate Solution will continue to push for additional commitments from other entities in support of future JV efforts.

APPENDIX C – SCENARIO

C.1. Scenario Design

In the scenario, the ACI wanted to (1) introduce effects that caused catastrophic damage on a single entity or organization; (2) have those effects spill over into another sector; and (3) eventually have the catastrophic effects reach multiple entities and organizations. This strategy allowed the ACI to examine the interdependencies and incident response gaps of the various critical infrastructure organizations participating in the experiment. Figure 17 is an illustration of the ACI's scenario development framework.



SCENARIO PHILOSOPHY

- Start small (locality and severity)
- Use injects which build on each other and in sequence to each other
- Introduce attribution late

1 Scenario effect causing catastrophic damage on a singe entity or organization
2 Catastrophic effects cross to another sector
3 Catastrophic effects across multiple entities or organizations

ENTITY
Single: One organization
Cross: Two organizations
Multi: Three or more

DAMAGE
Low: Internally inconvenient or not noticeable, no noticeable external effect
Medium: Internally disruptive, externally inconvenient
High: Internally destructive, externally disruptive
Catastrophic: Serious economic damage and/or some loss of life, serious disruption or damage to dependent organizations

Figure 17: JV 3.0 Scenario Development Framework

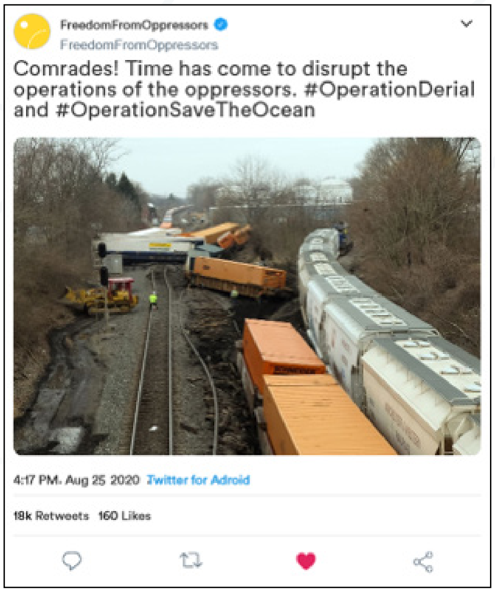
C.2. Scene Setter

For several days, heavier than normal spring rains have inundated the southeastern area of the Appalachian Plateau, causing widespread flooding in the area and regions to the south and east. Rivers are overflowing, resulting in over 44,000 being displaced in northern GA and western SC. Rivers are anticipated to remain high for the next several days. The governors of GA and SC have deployed the National Guard to their respective regions for humanitarian relief and the protection of infrastructure.

Meanwhile, the President of the United States has ordered the immediate and rapid deployment of two brigade combat teams to Europe to respond to aggressive actions taken by a geopolitical adversary of the United States. Within the international community, the civil conflict is largely viewed as a proxy war, with several ethnic factions opining publicly that foreign powers should stay out of the internal conflict. The local and global media are heavily covering the international dialogue, and several major powers with interests in the region would benefit from the United States remaining uninvolved. The U.S. secretary of state and secretary of defense have conducted a joint press conference, stating that the United States will rapidly deploy forces to the region to protect regional interests. In addition to combat troops, the President has ordered the deployment of defense systems, including vehicles, radars, missile systems, and other equipment, to support U.S. allies abroad.

Several Army battalions have been placed on alert for movement, and the forts and local community are aware that personnel and equipment are being deployed. The Army (Military Surface Deployment and Distribution Command [SDDC]) begins coordination activities to move vehicles and equipment from the local forts to the ports in Charleston, SC, and Savannah, GA. Most community residents know that troop and equipment movement is scheduled for September 22–24, 2020, though that is sensitive information. To support the summer offensive, the United States must have support to its allies by November 1, which necessitates departure from the United States by September 30 at the latest. Local news media has widely covered the local impact to communities because of the rapid deployment's large scale. Several activist groups have voiced strong opposition to the United States deploying troops to the region.

In addition, recently, DHS CISA released a preliminary alert that a new version of Emotet has been detected that indicates it can propagate via wireless networks. USCG has issued a maritime alert warning shippers, ports, and maritime facilities that the most recent version of Emotet malware is contaminating ships and maritime facilities globally, with over 43 new infections being discovered in vessels and port facilities. Within the past 6 months, U.S.-flagged vessels have been delayed entry into port four times because of widespread Emotet infections on their noncritical information systems. A Joint Intelligence Bulletin from DHS and the FBI highlighted disruptive ransomware attacks targeting the energy industry as an emerging concern.



FreedomFromOppressors
FreedomFromOppressors

Comrades! Time has come to disrupt the operations of the oppressors. #OperationDerial and #OperationSaveTheOcean

4:17 PM. Aug 25 2020 Twitter for Adroid

18k Retweets 160 Likes

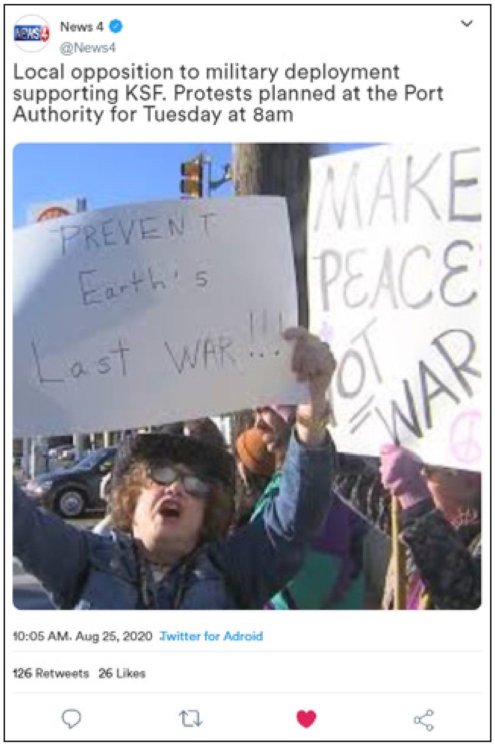
Figure 18: Domestic Terror Group Threat on Social Media

Furthermore, within the energy and utility sectors, Ryuk ransomware is being discussed often, and specific malware such as CrashOverRide and Triton continue to be of interest.

C.3. Turns 1–3 (ROC Drills and Preplay)

C.3.1. Turn 1

In turn 1 (Monday at 8 a.m.), the SDDC rapid deployment process has begun. The crews of several commercial cargo vessels report manifest system glitches. The main gate at the port terminal fails to open roughly once in every 20 attempts. As a solution, port security manually opens the gate, positioning additional personnel to do so. Meanwhile, electricity and natural gas utilities are experiencing phishing attempts. The FBI has issued a Private Industry Notification


News 4
@News4
Local opposition to military deployment supporting KSF. Protests planned at the Port Authority for Tuesday at 8am

10:05 AM. Aug 25, 2020 Twitter for Adroid
126 Retweets 26 Likes

Figure 19: Media Coverage of the Protest at the Military Terminal

about advanced persistent threats targeting the energy sector. In addition, the media is reporting that protests against U.S. involvement overseas will most likely be happening at the military terminal. Furthermore, domestic terror groups have threatened to derail SDDC's operations by posting a picture of a derailed train on social media.

C.3.2. Turn 2

In turn 2 (Monday at 5:47 p.m.), the public safety answering point is reporting a high volume of 911 ghosting calls. The electronic manifests of ship and rail cargo are being reported as inaccurate. Spam emails are being sent from SDDC email addresses. An energy security operations center has noted an uptick in suspicious emails and admitted that multiple employees in the human resources department have clicked on phishing links. In addition, a wireless router was discovered to have been installed in a traffic box. Port facilities are experiencing power voltage and quality fluctuations. Furthermore, the FBI has deemed the threats on social media from domestic terror groups as credible. Also, protests have begun at the military terminal, with the students and faculty of local high schools and colleges making up a large portion of the crowd.

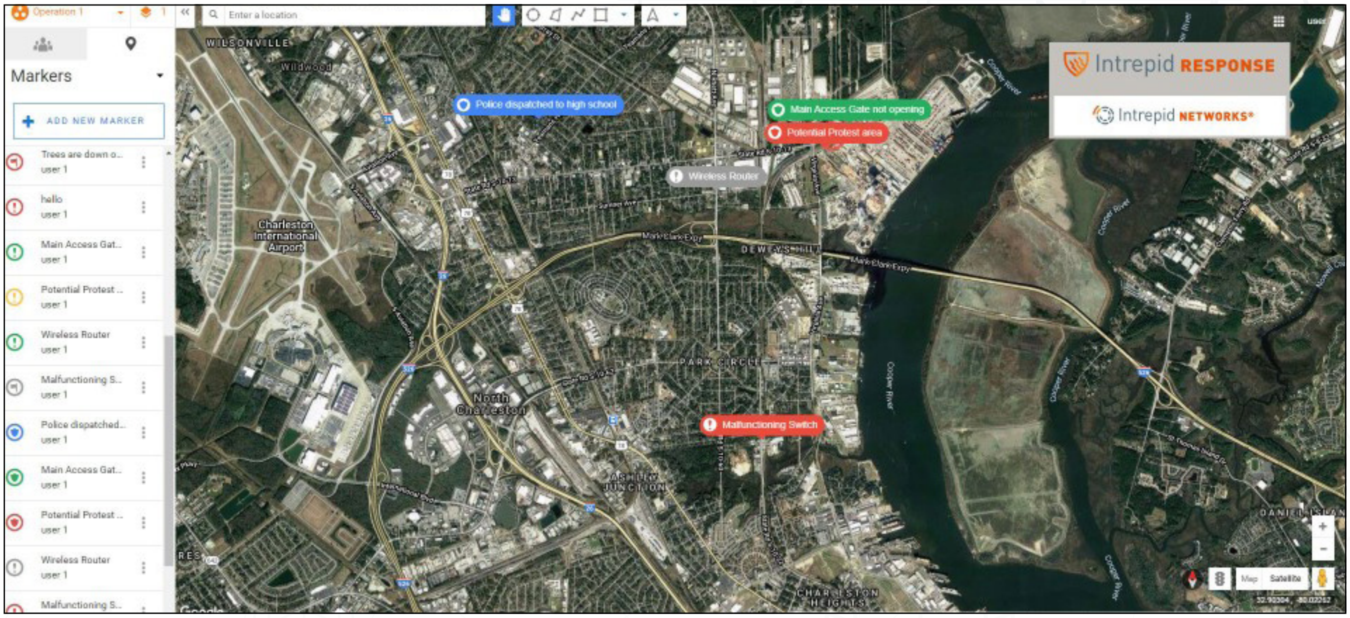


Figure 20: Turns 1–3 Common Operating Picture (Charleston)

C.3.3. Turn 3

In turn 3 (Tuesday at 7:21 a.m.), 911 call centers are struggling to manage incoming calls because the 911 ghosting has become overwhelming. The electronic manifests of ship and rail cargo are still inaccurate, and the port database has been discovered to be corrupted as well. In addition, the access database for entry into the port has been corrupted; as a result, the backup system has been implemented. The spam emails from SDDC email addresses are increasing in volume. The malware Emotet has been detected on ships heading for the port, and the FBI has confirmed two of these cases. Furthermore, a malfunction has occurred at a major rail switching station. Also, Department of Transportation crews are investigating instances of possible sign and light tampering, but the crews have come to no conclusions yet.

C.4. Turns 4–7 (JV 3.0 Exercise Main Play)

C.4.1. Turn 4

In turn 4 (Tuesday at 3:42 p.m.), the discovery has been made that natural gas utility remote terminal unit firmware does not match the latest patch from the vendor. The energy information sharing and analysis center has issued a traffic light protocol of "AMBER" because of credible cyber threats. Port and local law enforcement are coordinating to monitor the protests. Protesters are livestreaming, and the protests have garnered international media attention. Emails purportedly from the Port Authority are sending past-due invoice emails to electricity utility employees. Electricity and natural gas utilities are worried that their automated pay systems will fail to pay employees on payday. In addition, SDDC's Integrated Computerized Deployment System (ICODES) is suffering from constant glitches. A power plant night-shift manager believes his cursor was moving by itself. Port properties are experiencing vandalism, including graffiti and broken windows. Furthermore, the denial-of-service attack is ongoing at the 911 call center. Also, traffic is becoming a problem; with lights and signs being manipulated, trucks attempting to enter the city are backed up on streets and highways.

Figure 21: Trucks Entering the City Are Backed Up on the Highway

C.4.2. Turn 5

In turn 5 (Tuesday 10:58 p.m.), a major voltage drop has occurred at an electricity distribution substation serving the city, and three natural gas compression stations serving the city have experienced depressurization. Loss in pressure has led to a drop in electrical output at the power plant, which has activated backup fuel reserves. Elsewhere, the local police department is now experiencing ghosting calls. Media are flooding the mayor's office, seeking information and comment. In addition, a freight truck has lost control and crashed into multiple vehicles on I-95, causing a massive backup in traffic. Traffic is being diverted off the interstate.

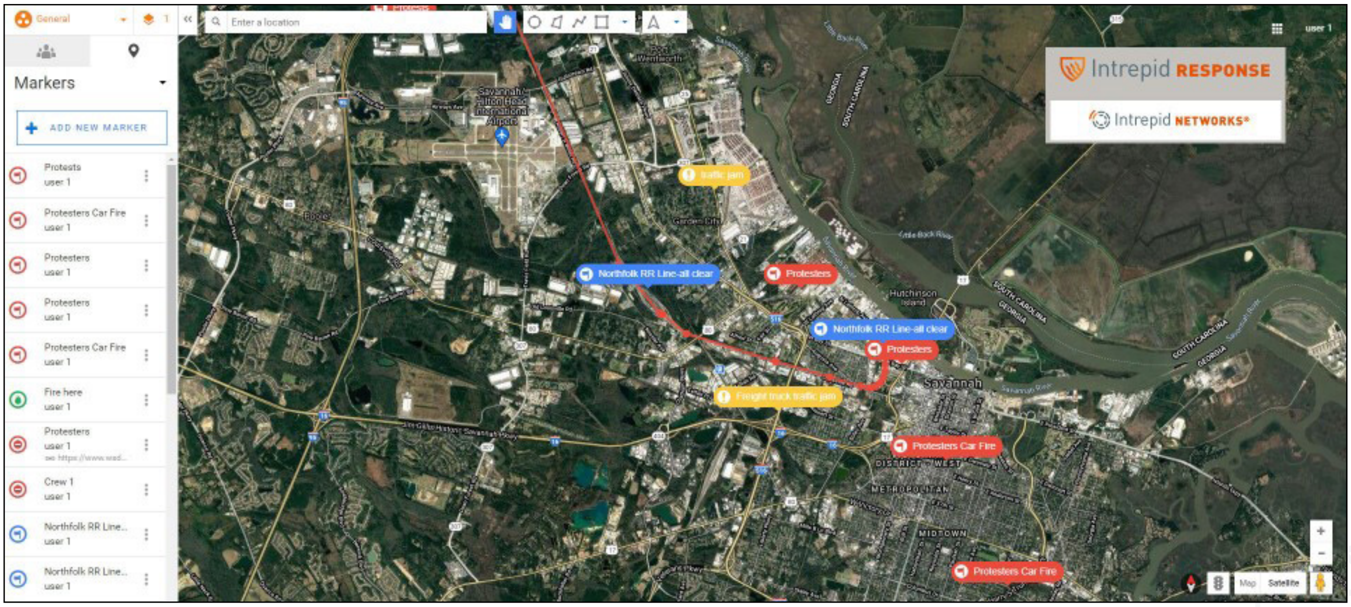


Figure 22: Turn 5 Common Operating Picture (Savannah)

C.4.3. Turn 6

In turn 6 (Wednesday at 8:14 a.m.), a ship has listed (i.e., tilted) and dumped 52 cargo containers (not including military equipment) onto the pier and into the adjacent water. The port has closed pending an investigation into the cause of the malfunction; investigators are attempting to ascertain if hazardous materials were in the containers. Meanwhile, ICODES is completely nonfunctional. Two more freight trucks have stalled, this time in city intersections; the drivers are reporting that their engines "just shut off." Two protective relays at relay stations servicing the port and the local hospital have taken uncommanded actions; apparently, this was the result of a sensor failure. In addition, the security operations center has discovered indicators of compromise on utilities' OT systems.

C.4.4. Turn 7

In turn 7 (Wednesday at 6:10 p.m.), USCG and the Port Authority are still investigating the reason the cargo ship listed. With port access closed, rail, freight, and shipping have been severely impacted. In addition, a water treatment plant has experienced power failure, and the local school district has no running water as a result. Backup power at the port has been inconsistent. The energy utility has confirmed that its human resources system has been infected with Ryuk malware ushered in by Emotet. Furthermore, the city traffic system has been hit with ransomware that appears to be localized to the city traffic network.

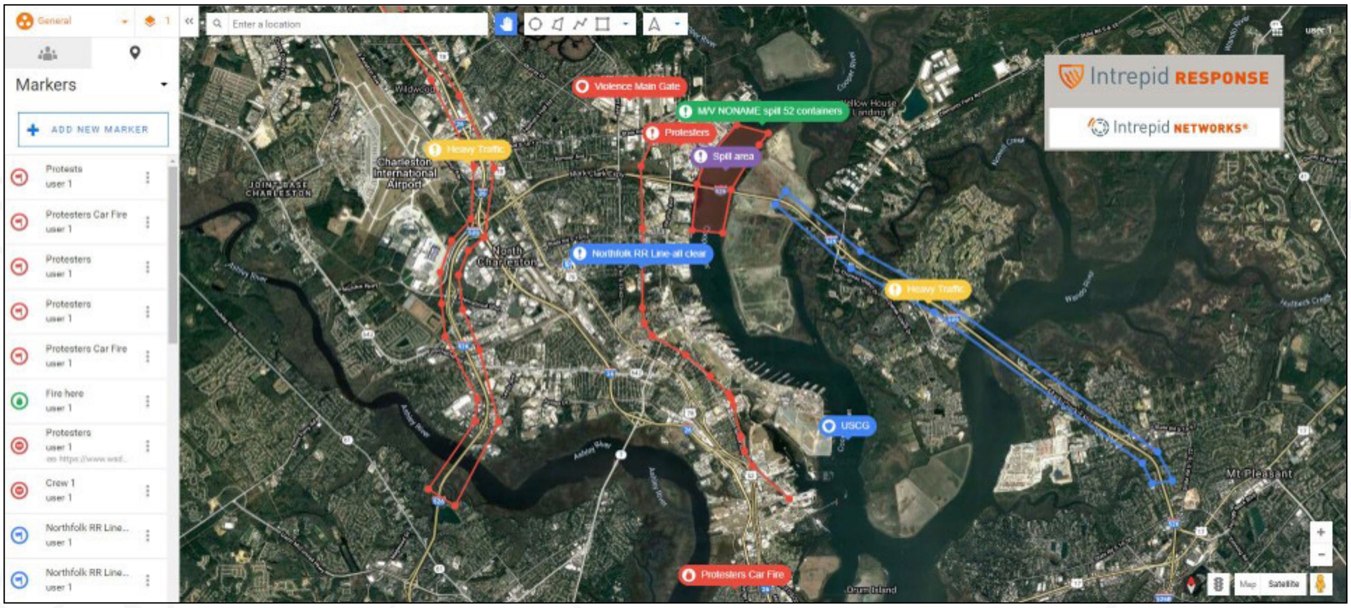


Figure 23: Turn 7 Common Operating Picture (Charleston)

APPENDIX D – LAW/POLICY TABLETOP EXERCISE (TTX)

Law/Policy TTX

The Law/Policy TTX was a planning workshop and mock exercise that occurred February 18–20, 2020. The first two days consisted of presentations by the ACI and various partners and critical infrastructure stakeholders from SC, GA, the federal government, and private industry, and the third day consisted of a mock exercise that covered turns 1–4 of the JV 3.0 exercise.

The goals of the Law/Policy TTX were to:

- Identify support required at the municipality level and below;
- Stress cross-jurisdictional information sharing;
- Determine third-party support prioritization;
- Identify thresholds for business continuity without the availability of technology;
- Improve information sharing and discuss how to defeat misinformation; and
- Set JV 3.0 up for success.

Day one of the Law/Policy TTX focused on partnerships. The ACI discussed the JV 3.0 scenario, stating that the intended effect was to have participants respond to a cybersecurity incident and then analyze their response, asking themselves whether the response would be effective, whether it was realistic, would there be obstacles to the execution of the response, and with whom they should coordinate in executing the response. Specific goals that were mentioned included improving cyber coordination among the JV participants and promoting the JV exercise overall. The importance of utilizing available federal cybersecurity resources was emphasized. In addition, the ACI encouraged participants to exchange contact information so that they would be better prepared for a genuine cyber incident.

The ACI gave an overview of the JV project as whole. The institute stated that past exercises indicated that JV participants were generally not prepared for a cyber incident. The institute emphasized the importance of cybersecurity exercises and noted that a major goal of JV is to establish a cyber framework based on lessons learned from past JV iterations. The ACI noted that though it is a major step forward for cities to devote time and resources toward establishing a cyber command, cybersecurity exercises are essential if cyber commands are to be prepared for real-life cyber incidents. Other goals mentioned included helping cities with their critical infrastructure; helping cities identify available financial and personnel resources; and studying the likely effects of a cyber, physical, and informational attack on a port city.

Yet another goal discussed by the ACI was advancing cities' understanding of the constraints, restrictions, and opportunities of municipal and federal law as they apply to the cities' cyber incident response plans. For example, a city must understand Title 32 authorities, how they may be used to support cyber incident response, and their limitations in supporting a city's response. Organizations must also be aware of the Antideficiency Act and the limitations of organizations' roles in cyber incident response. The institute emphasized the importance of developing a team approach to cyber incident response and eliminating information silos, which may be created by laws, policies, attempts to preserve the good reputations of organizations, and questioning the "need to know" of others. The institute noted that though information sharing is necessary for a response plan, it is not sufficient; the information must be used to drive timely, relevant decision making.

Next, the importance of partnerships was discussed. The discussion emphasized the importance of information sharing among public organizations, among private organizations, and between public and private organizations. When organizations share information, they see cybersecurity from each other's points of view, helping to foster a more comprehensive, collaborative, shared understanding of cybersecurity. However, there are obstacles to cyber information sharing: An individual may not have the appropriate security clearance, and organizations' legal agreements may prevent certain information from being shared.

In addition, organizations must identify the partners who would be the most valuable in the case of a cyber incident. If two organizations share the same goal, they may wish to partner with each other, even if they belong to two separate sectors altogether. The importance of maintaining partnerships through quarterly meetings, dial-in meetings, and/or brown-bag lunches was emphasized.

Day two of the Law/Policy TTX focused on planning and leader training. Day two saw the ACI provide a more in-depth discussion of cyber incident response. The institute discussed the following vital steps:

- Performing a risk assessment;
- Prioritizing security issues;
- Creating a communications plan;
- Monitoring the network to identify cybersecurity breaches;
- Gathering information on incidents when they occur;
- Identifying the organizations that have the authority to address the cyber incident;
- Identifying thresholds for notifying external organizations of the incident;
- Containing and isolating the incident;
- Investigating the cause of the incident;
- Recovering from the incident;
- Determining an appropriate time period for testing; and
- Identifying lessons learned from the incident.

Next, the institute discussed the vital components of a cyber response plan. These include support from management and accounting, balancing the degree of detail with the degree of flexibility, knowing the organization's stakeholders, and keeping the plan simple.

On day three of the Law/Policy TTX, a mock exercise was held that consisted of turns 1–4 of the scenario. The goal of the mock exercise was to refine the exercise scenario and maximize its usefulness to participants.

Execution TTXs

Over 200 individuals and over 60 organizations participated in the JV 3.0 exercise TTXs on September 22 and 24, 2020. Because the Charleston and Savannah exercises had been compressed into single, 1-day events, time only permitted turns 4–7 to be executed. Participants utilized the DECIDE® platform to receive scenario injects and Microsoft Teams to communicate across the tables containing the representatives from the respective industries and sectors (for example, DoD, non-DoD, and the energy sector).

ACI's TTX facilitator asked discussion questions about participants' hypothetical reactions to the scenario, whom they would contact, how they would be sharing information about the incident, the legal authorities that would govern their responses, and authorities that do not exist but would be helpful in the given scenario. The questions were usually directed at specific tables so the ACI could ascertain the actions that the given sector would be taking (or not taking) in response to the injects. The questions led to discussions among participants about their respective organizations' capabilities, legal authorities, incident response plans, etc.

Following the TTXs, the ACI conducted an After Action Review; debriefed participants; and encouraged them to continue to stay engaged, network with one another, and analyze their organizations' capabilities to prepare for a Cyber Worst Day scenario.

APPENDIX E – LIVE-FIRE EXERCISE

The LFX is a JV exercise component that uses an on-range, simulated, virtual environment. The LFX follows a scenario that correlates with the TTX scenario. It exposes participants to threat tactics, tools, and shared techniques and tests cyber equipment and response capabilities in real time. Though it is an integral part of JV, it was canceled for JV 3.0 because of issues arising from the COVID-19 pandemic.

In a cyberattack simulation such as JV, a realistic training environment is key to the exercise's success. In the LFX, the on-range network, virtual range environment emulates critical infrastructure environments to enhance training. The LFX pits two teams of technical analysts and operators—a Red Team (attackers) and a Blue Team (defenders)—against each other in various scenarios. In the exercise, the opposing forces and scripted injects attack participants' networks. The LFX demonstrates the impacts of successful attacks and allows defenders to exercise their cybersecurity skills in an operational environment.

The sophistication of the LFX virtual environment varies based on available capability. The LFX aims to examine and validate coordination and command and control among various multiagency coordination centers, such as emergency operation centers. The tactics, techniques, and procedures employed during the LFX follow an exercise plan that includes a list of equipment and unit control measures, including means of communication.

The intention for JV 3.0 was to develop customized virtual networks that mimicked the architecture and behavior of each participant organization (e.g., the City of Charleston or SDDC). This was to be achieved by coordinating with each participant organization to determine the priority and level of detail to be included in the virtualized network and developing distinct yet integrated organizational virtual network enclaves.

To the degree possible, the cyber range was to include virtual hosts and networks that mimicked the relevant portions of the IT systems participants use on a daily basis. Specifically, network architectures, the numbers and types of hosts, and the software platforms of participants were to be incorporated into the cyber range. The network tools and business software were to include enterprise resource planning software (for human resources and accounting); network file sharing and accounts; and human-machine interfaces for city traffic, power infrastructure, Port Authority operations, and transportation of goods to and from ports by truck and rail, allowing participants to read sensor output and track activity. For example, participants would be able to interface with ICODES, which would display a warning when a ship was about to list (see figure 24).[44] One important aspect was that the virtual range and the physical range were to affect one another in the exercise to create a realistic and holistic experience. For example, the effects of an attack on physical devices would have been reflected in the information provided to participants or would have affected their ability to perform a specific task.

[44] "ICODES Upgrades to Enhance Military Distribution and Deployment Processes for Joint Services," Tapestry Solutions (website), August 18, 2017, https://www.tapestrysolutions.com/2017/08/18/icodes-upgrades-enhance-military-distribution-deployment-processes-joint-services/.

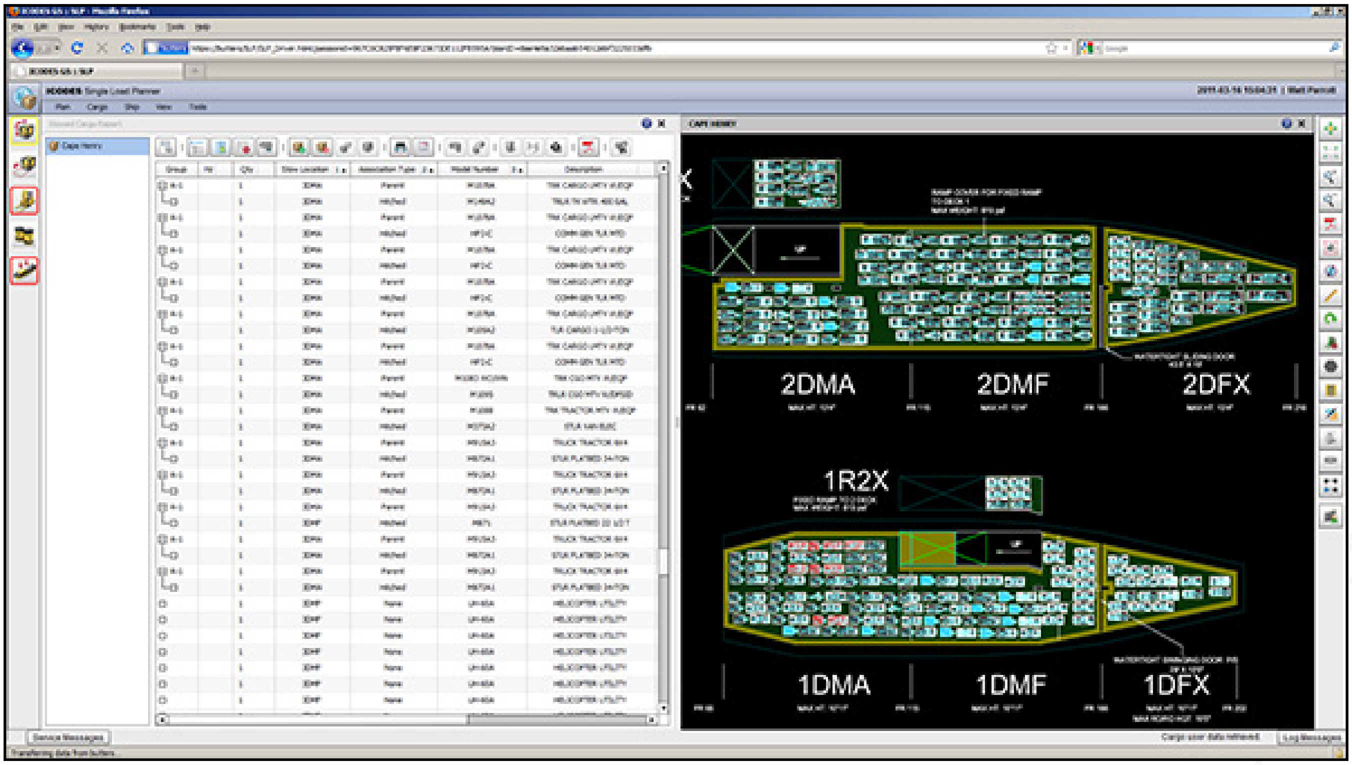


Figure 24: Participants would have received a warning in ICODES if a ship was about to list.

All of the participating organizations' networks were to be integrated into a holistic network that imitated the Internet. Participants from one sector (e.g., energy) would have been able to communicate with participants from another sector (e.g., Port Authority) using standard Internet working protocols. This component is vital because participants from different sectors need to be able to contact one another in their attempts to mitigate the impacts of the physical or virtual crises they are encountering. After all, one of the goals of JV is to encourage participants from different sectors to interact with one another; observe the interdependencies among various sectors; and survey other organizations' roles, responsibilities, strategies, and capabilities.

APPENDIX F – MILITARY TESTIMONIALS

F.1. 3rd Infantry Division (3ID)

Force projection is the movement of personnel and equipment from one location to the next in direct support of defined operational objectives. In the contextual framework of JV, participating members of the cyber community work to enable military commanders in the accomplishment of their objectives while being obstructed by numerous cascading obstructions.

As members of the Savannah-area community, 3ID is dependent upon government and private partners in the area to accomplish day-to-day operations and fort-to-port movement. Soldiers and civilians that work on Fort Stewart are also citizens of the Savannah area community. In this way, JV demonstrates that adversarial activities in cyberspace can have impacts across the community and affect operational and strategic objectives. JV contributed to a shared understanding of these dependencies among 3ID and Fort Stewart movement planners and emergency managers.

Broadly, 3ID uses stationary networks on Fort Stewart for day-to-day operations—either strategic networks owned by 7th Signal Command or home-station mission command networks owned by 3ID. 3ID also has deployable network capabilities from the Warfighter Information Network-Tactical line of capabilities. 3ID protects the tactical network with Cyber Network Defense and Network Operations Security Center tools.

The primary lesson 3ID learned in JV is dependency analysis, also known as cyberspace terrain analysis, leads to better risk awareness. A general dependency analysis helps understand how information systems enable the division to accomplish its mission and how an adversary might affect that mission. Cyberspace terrain analysis describes the division's cyberspace terrain with links between information systems, networks, staff processes, and operations. 3ID is incorporating this type of dependency analysis in preparation for Army Warfighter Exercise 21-3.[45]

3ID's Force Projection Posture: The rest of the discussion uses these four phases of force projection:

- Phase 1: Predeployment Activities—Predeployment activities are training, day-to-day operations, equipment staging, and movement coordination.
- Phase 2: Fort-to-Port Movement—Fort-to-port movement is the movement of 3ID equipment from Fort Stewart to the port of Savannah and embarkation on vessels.
- Phase 3: Port-to-Port Movement—Port-to-port movement is the movement of 3ID equipment from port of Savannah to some distant port.
- Phase 4: Port-to-Assembly Area—Port-to-assembly area is the disembarkation and movement to a precombat staging area.

[45] U.S. Army Combined Arms Center, "The Warfighter Exercise" (PowerPoint presentation, Mission Command Training Program Orientation, Fort Leavenworth, Kansas, October 16, 2017), https://usacac.army.mil/sites/default/files/documents/cact/mctp/The%20Warfighter%20Exercise.pdf; and U.S. Army, "America's First Corps Completes WFX 20-3," U.S. Army (website), February 13, 2020, https://www.army.mil/article/232744/americas_first_corps_completes_wfx_20_3.

The scope of JV, with respect to 3ID's mission, is the second phase—the narrow window of an armored brigade combat team's movement between Fort Stewart and the port of Savannah. 3ID trains and deploys a lethal armor division as part of a joint force. Much of the movement associated with this mission is outsourced to other entities, especially in phases 2 and 3. The division transportation officer and his or her staff coordinate with SDDC and the local Army Field Support Battalion to plan and execute movements. This coordination is largely done using garrison unclassified networks and SDDC's ICODES. Additional coordination uses unclassified enterprise email and Voice over Internet Protocol.

In a tactical operation, 3ID defends the networks it owns that enable the mission, but phases 2 and 3 are not enabled by 3ID-owned cyberspace. In phase 4 and beyond, 3ID would employ tactical networks that might very well be vulnerable and under threat. 3ID would be responsible for mitigating these risks with assets it owns. 3ID does not have the authority nor the capacity to assist non-3ID entities in cyberspace. In essence, 3ID would be impacted by cyberattacks against civilian infrastructure during phases 2 and 3, but could not directly defend against these types of attacks.

In contrast, in phase 4, 3ID would employ mostly tactical networks in the port-to-assembly area movement and still be quite dependent on civilian infrastructure in friendly terrain. For instance, contracted carriers may be used for some equipment, but that coordination would be much less outsourced (i.e., contracted from the division instead of SDDC). In this case, 3ID would defend its cyber terrain against direct cyberattack while also staying aware of threats against civilian cyber terrain. JV showed 3ID the importance of understanding these sorts of dependencies from a risk analysis perspective.

Adjusting Analysis Frameworks and Other Lessons Learned: The primary lesson 3ID took away from JV is the complexity of dependencies. 3ID's goal in cyber defense strategy is to develop a prioritized defended asset list and prepare to rapidly assess the impacts of a cyberattack on its mission. 3ID uses three frameworks to describe cyberspace terrain: Joint Publication 3-12 cyberspace layers; Army Doctrine Publication 3-0's operational framework; and Army Protection Plan, Army Regulation 525-2's Mission Essential Function (MEF).[46]

Joint Publication 3-12, Cyberspace Operations, describes cyberspaces terrain in three layers: (1) *persona layer* contains the mission, commander's guidance, operational lines of operations and effort, and other artifacts that describe the operational framework; (2) the *logical layer* is the software and protocols that information networks and systems use to communicate; and (3) the *physical layer* is the set of devices and communication medium that make up information networks. Describing the cyberspace terrain at 3ID during a mission means describing the components of the information networks and systems (physical); how they are connected (physical, logical); how they process and pass information (logical); and how personnel and activities use the information to accomplish the mission (persona).

During the JV 3.0 exercise, 3ID found it helpful to use additional frameworks to further describe the cyberspace layers to show how the cyberspace terrain enables and affects the division's mission. The operational framework, described in ADP 3.0, *Unified Land Operations,* describes an area of operations

[46] Joint Chiefs of Staff, Cyberspace Operations, Joint Publication 3-12 (Washington, DC: Joint Chiefs of Staff, February 5, 2013); Department of the Army, *Unified Land Operations*, Army Doctrine Publication 3-0 (Washington, DC: Department of the Army, October 2017); and Headquarters, Department of the Army, *The Army Protection Program*, Army Regulation 525-2 (Washington, DC: Headquarters, Department of the Army, December 8, 2014).

with deep, close, support, and consolidation areas; the decisive, shaping, and sustaining operations; and main and effort. The operational framework is a natural way to describe each layer of cyberspace terrain aligned with the operation, but it has limited ability in prioritizing cyber defense assets.

The MEF from Army Regulation 525-2, *The Army Protection Program*, describes generalized activities at the division headquarters. Discretely linking information systems in the logical and physical layers to MEFs enables more intuitive prioritization of defense assets. Prioritizing MEFs also sequences the systems that support them, further supporting a more holistic understanding of how cyberattacks affect a given MEF.

In the JV 3.0 exercise, one such specified MEF for 3ID was “coordinate movement.” Supported information systems included unclassified garrison workstations, networks, and ICODES software. This MEF persisted between all operational phases because the division needed to coordinate its movement throughout the scenario. However, even with “coordinate movement” remaining a priority in phases 1 and 2, these systems were outside 3ID’s defended list. As a result, JV 3.0 demonstrated that an adversary can also effectively impact division MEFs indirectly through cyber avenues of approach.

F.2. Military Surface Deployment and Distribution Command (SDDC)

For SDDC and United States Transportation Command (USTRANSCOM), force projection is integral to global port readiness. The command’s support to surface force projection is its ability to project power anywhere in the world.

This power projection starts in the continental United States and depends on traditional transportation methods that connect ports and strategic locations. It is a large system that relies significantly upon the support of its local partners.

To assess readiness, USTRANSCOM reviews its capacity to manage power competition and the cargo demands and access vulnerabilities that its most strategic ports face. Most recently, this review of the United States’ force projection includes cyber activity that could limit the country’s ability to operate. With a congested cyberspace domain, adversaries frequently attempt to degrade U.S. force projection, making cyber missions a top priority. USTRANSCOM drafted a Cyber Domain Mission Assurance Strategy to outline its actions to increase cybersecurity and incorporate cyber protection in its force projection goals and objectives. This directly helps its Joint Deployment and Distribution Enterprise mission,[47] which ensures USTRANSCOM’s ability to expand its use of seaports in the United States and abroad.

To align with USTRANSCOM’s cyber domain mission assurance strategy and Joint Deployment and Distribution Enterprise, SDDC’s strategic readiness for port diversification includes maintaining global deployment networks, mobility capacity, and the global command and control necessary to respond immediately with forces. SDDC assesses its strategic readiness by identifying and using mission-critical seaports for brigade-sized deployments in preparation for large-scale combat operations around the world. Exercising this domain across all combatant commands allows SDDC to practice its ability to swiftly dispatch forces anywhere in the world and establishes relationships with allies and partners well before a crisis. JV provided an opportunity to put pressure on SDDC’s systems and readiness.

[47] Joint Chiefs of Staff, *Distribution Operations*, Joint Publication 4-09 (Washington, DC: Joint Chiefs of Staff, February 5, 2010).

SDDC Force Projection during JV 3.0

During the exercises, SDDC's Surface Operations Center was in charge of managing force projection for the port/port operations and federal sectors during JV. At the beginning of the exercise, the scenario involved aggressive actions taken by a geopolitical adversary of the United States. To respond to these actions, the U.S. government ordered deployment of brigade combat teams to Europe and sent combat troops, defense systems, and other equipment to support U.S. allies abroad. Then, SDDC began its involvement, starting with coordination to move vehicles and equipment from the local forts to ports in Charleston and Savannah. The Surface Operations Center battle captain led the team as they monitored all major departing and arriving cargo movements at every port.

SDDC's global network capabilities were tested heavily during the exercises, with Emotet-infected ship cargo manifests, malfunctioning major rail switching stations, and rampant phishing attempts. For example, during turn 4, SDDC's ICODES system was glitching, showing inaccurate manifests. In this scenario, SDDC recommended contacting the ICODES program manager to determine whether the system is affected at the host location and alert the ICODES team to begin solving the corruption problem with ICODES and other utility OT systems. In the meantime, SDDC started to track cargo manually.

SDDC's most pertinent recommendation throughout both Savannah and Charleston's exercises was to change locations for rapid deployment of equipment and move all cargo and port operations to another port. In particular, during the turn 7 inject, trucks began to stop on their own volition, interstates were being shut down, and Port Authorities had suspended port operations along the Eastern Seaboard because of cyberattacks. During the turn 7 scenario, SDDC stated that, if necessary, it would deploy reserve components and work with state authorities and the National Guard to use rapid port opening elements, transportation units, and wrecker and maintenance units for stranded cargo loads. In addition, SDDC reserve components would provide support measures to help move cargo from the interstate to the port using commercial trailers or otherwise transload all cargo. SDDC would communicate with the 597th and 598th Transportation Brigades, the Joint Chiefs of Staff's Director for Operations, and other receiving units to provide cargo status updates and any delays.

Lessons Learned from JV 3.0

Through completing the JV exercise, the battle captain gained a greater awareness of the effects that cyber incidents have on one port. SDDC also determined that the most successful incident responses resulted from each sector having prepared emergency response protocols outlined for most of the situations that occurred during the exercise and instances in which coordination between the different sectors and agencies had been developed prior to the exercise. Essentially, a whole-of-community approach among all sectors becomes critical in situations like those in JV.

The battalion commander also suggested adding JV to the SDDC commander's course. The battalion commander said an exercise like JV would add value for the leaders of transportation brigades, bring awareness to important port assets, and provide specific challenges that are not addressed in other brigade commander training courses.

Also, more exercises like JV will allow SDDC to analyze further the impact of a cyberattack against critical force projection infrastructure and test the strength of its cyber incident response plan. With SDDC having recently migrated 100 percent of its surface transportation business systems into its cloud system, digital modernization and cyber mission assurance have become more important than ever in SDDC's mission, port diversification efforts, and force projection readiness.

Other findings by SDDC included the following:

- Rail
  - For rail input, SDDC used four trains with 50 cars per train totaling 600 pieces delivered over a period of 1 week.
  - Only 2 days' worth of data were analyzed, so two trains that were notionally scheduled over the 2 days of JV exercises were projected to deliver 240 pieces. One train being delayed or stopped prevented 120 pieces of cargo from making it to the port.
- Commercial line haul
  - One hundred to 150 trucks that were notionally scheduled over the Defender 2020 exercise were divided to meet the 2-day JV exercise scenario, so 20 trucks a day being delayed or stopped prevented 100 pieces of cargo from making it to the port.
- Military convoy
  - The military convoy from Fort Stewart consisted of 20 serials / 1,200 pieces, roughly equaling 60 pieces per serial. This would result in 60 pieces of cargo being delayed or stopped on its way to the port.
- Summary of impacts
  - Two hundred eighty pieces would have been delayed, stopped, or not made it to the port over the 2-day period. In addition, two trains and an unknown number of military convoys would have been stopped, and several line haul moves would have occurred.

APPENDIX G – PRIVATE INDUSTRY TESTIMONIALS

G1. Intrepid Response

Intrepid Response is a simple-to-use and affordable, mission-critical, mobile and web-based software solution that enables instant team communication, coordination, and collaboration over a common operating picture. It is uniquely designed to support the day-to-day operations of users in the field as well as incident/emergency management, base security, and surveillance operations. Intrepid Response can integrate with strategic-layer tools that would be found in a command and/or operations center. The software can operate with any cellular network, including Verizon, AT&T, etc. Intrepid Response is the only application of its kind that is FirstNet-certified for public safety, meaning it meets stringent requirements for usability, security, reliability and availability. As such, the application can be utilized in scenarios in which user priority and preemption are enabled.

Figure 25: Intrepid Response is a user-friendly situational awareness system comprised of Android/iOS smartphone and web-based applications.

Intrepid Response is a user-friendly shared situational awareness system that comprises Android/iOS smartphone and web-based applications. The ecosystem provides an integrated suite of capability that comprises real-time geospatial data, emergency notifications, push-to-talk voice communications, and multimedia sharing for resource management, team collaboration, and incident management. The platform may be deployed on a customer-hosted on-premise server or via secure cloud-hosted solutions, including Amazon Web Services GovCloud. The mobile platform creates a real-time common operating picture for tactical and supervisory units while integrating with strategic tools for top-to-bottom command and control. The Intrepid Response platform supports all major operating systems, including native applications for both iOS and Android, plus browser apps for all significant modern browsers (Chrome, Internet Explorer 11, Edge, Firefox, and Safari).

Intrepid Networks was invited to participate in the JV 3.0 exercise as an industry partner to provide its situational awareness and collaboration platform, Intrepid Response, for participants to utilize during the decision-making process. Intrepid Networks' FirstNet-certified Intrepid Response platform provided a common operating picture and the ability to exchange information in real time across federal, state, and local government and civilian participants. For the JV 3.0 exercise, Intrepid Response provided a turn-by-turn common operating picture of events unfolding as a result of organized cyberattacks in the cities of Charleston and Savannah, providing visualization of valuable data over the Intrepid Response common operating picture to participants instantly, without the added latency of manual interpretation and relay. This capability is a key enabler of more rapid and accurate decision making; dispatch; and response communication, coordination, and collaboration. The capability ensures a more effective response and more timely recognition of seemingly random events as being related (or not related) to an organized and persistent cyberattack.

Situational awareness is a concept that military personnel have discussed and been trained on for decades. Numerous definitions, books, dissertations, and white papers have been published on the concept. For its observations, Intrepid Networks utilized the framework of “perception, comprehension, projection, and prediction,” as discussed in the report Defining and Measuring Shared Situational Awareness by Albert Nofi.[48]

For the sake of clarity, perception, comprehension, projection, and prediction are defined below:

- Perception: Gathering information that is available.
- Comprehension: Understanding the information gathered and the impacts it has on one’s domain.
- Projection: Estimating how a situation will evolve in the future.
- Prediction: Evaluating how other forces or events may impact one’s projection.

Intrepid Networks’ observed results are discussed below from the shared situational awareness perspective.

G.1.1. Findings

Intrepid Networks’ observations were gathered during the JV participants’ discussion and decision-making sessions that occurred throughout the experiment. Intrepid Networks intended to observe how decision-making processes may evolve while utilizing a common operating picture and collaboration platform. As a result of the exercise transitioning to a virtual venue due to COVID-19, Intrepid Networks pivoted from providing live mobile and web application access to participants for communication, collaboration, and coordination to providing static map images that evolved as the exercise proceeded. Intrepid Networks’ observations revealed that even these static map images provided a valuable means for participants to perceive; comprehend; project; and, to some extent, predict outcomes based on the variables realized in the earlier processes. Table 7 lists some issues encountered during the JV 3.0 exercise, Intrepid Networks’ observations, and Intrepid Response capabilities that can address these issues.

[48] Albert A. Nofi, *Defining and Measuring Shared Situational Awareness* (Alexandria, VA: Center for Naval Analyses, November 2000).

Issue	Exercise Observation	Intrepid Response Capability
High variation in tactics, policies, and procedures	Currently, there is high variation in the tactics, policies, and procedures of the various organizations that must collaborate to recognize and respond to an attack. In addition, these tactics, policies, and procedures are very manual and labor-intensive. Tools are needed to streamline, automate, and codify workflows.	Can be tailored to automate critical workflows to significantly reduce waste (in terms of errors, human resources, and cycle time) and improve effectiveness and safety.
Cycle time to diagnose attack	Currently, disparate organizations do not have a common operating picture of events within and outside their domains. Tools are needed for faster recognition that seemingly disparate events across different domains of responsibility are related to (or not related to) an organized cyberattack.	Provides layered information over an uncluttered common operating picture across disparate organizations that makes patterns and connections between these seemingly unconnected events obvious.
Coordination of response forces	Currently, disparate organizations lack the tools to launch coordinated efforts across disparate federal, state, and local organizations, all of which need to interoperate. Real-time communication, information capture and exchange, and mapping for more rapid and effective dispatch efforts are critical for operational success.	Provides the ability to quickly and accurately dispatch disparate response teams and enables these teams at the edge to securely communicate, collaborate, and coordinate over the common operating picture and with the command center.
Battle damage assessment	Currently, there is no apparent, common way to capture and share after action reports as part of a national strategy for continuous improvement in the Nation's ability to identify and respond to an attack. Efforts are needed to define such a format and codify it into an automated tool.	Can be readily enhanced to produce after action reports in a well-understood format tailored to support such a national strategy.

Table 7: Issues, Observations, and Intrepid Response Capabilities

G.1.2. Analysis

Intrepid Response provides a flexible platform that enables disparate, cross-domain entities to enhance to the situational awareness loop, both individually and collectively. Intrepid Networks' observations led to the conclusion that a true common operating picture is achievable in cybersecurity response operations by providing a means for cross-domain entities to connect seemingly disparate cybersecurity issues (perception) to a larger, coordinated cyber threat (comprehension). This leads to a more informed response posture, both at the organizational and collective, cross-domain levels (projection and prediction). Ultimately, the Intrepid Response platform expedites activities such as dispatching a particular unit to a threat and, as such, garners a more holistic, cross-domain cyber threat response while tightening the communication loop between organizations. Intrepid Response significantly increases the ability to effectively and efficiently respond to cyberattacks and allows organizations to minimize damage and chaos.

While Intrepid Response enhances situational awareness and collaboration, reducing the impact of cyberattacks, Intrepid Networks recognizes improvements to the platform would provide an even more seamless cross-domain cyber threat response tool that would allow its teams to evolve as our adversaries' capabilities improve. Intrepid Response provides a flexible, upgradeable platform that can be used out of the box today, but it can be updated to provide increased capability as it becomes available. Intrepid Networks has identified the following features that would evolve Intrepid Response to meet near-term needs for its cyber response teams:

1. Federating channels and/or organizations to provide more rapid information sharing, whether geospatial or specific documentation. This may be realized with an approach that many commercial interteam/intrateam communication tools take, such as providing common workspaces that any organization with a proper invitation may join. This approach would also prevent the ubiquitous "data fog" found in today's digital era.
2. Visualizing network- and cyber-related issues and threats on the map to further increase the capability for perception and comprehension in the situational awareness loop. As an example, enhancements can be made to allow for user-friendly input and visualization of vulnerable cyber elements in a geographic area of interest, such as wireless network systems, strategic servers, infrastructure supervisory control and data acquisition (SCADA) systems, etc., to get a snapshot view of location and other key information about this type of strategic infrastructure vulnerable to cyberattack.
3. Providing a mechanism for the Intrepid Response map to ingest layers from disparate geospatial systems (for example, traffic light or electrical grid statuses). This would further contribute to a true common operating picture for cross-domain cyber threat responses (expedite perception, comprehension, projection, and prediction).
4. Integrating data analytics into the Intrepid Response platform for improved automated recognition of a coordinated attack.
5. Implementing an automated after-action reporting feature that is tailored to a nationally accepted format to allow for continuous information sharing; evaluations; and improvements to tactics, policies, and procedures across disparate organizations in various areas of the country.

APPENDIX H – ALL HAZARDS ANALYSIS (AHA)

Idaho National Laboratory's (INL's) AHA tool is a hybrid data and expert knowledge management system that enhances situational awareness and decision making by enabling the development of function-based infrastructure dependency models. The INL team supported the JV 3.0 and Jack Pandemus exercises by using its AHA tool to process open-source government information, regulatory information, and other publicly available data to develop dependency models for the Charleston and Savannah regions, and then performing dependency analyses for these regions. INL created an instance of AHA for the JV exercises and loaded the results of the analysis into it. The JV instance of AHA was utilized to create cascading-impact scenarios that highlighted downstream impacts resulting from the degraded operations at various infrastructure in the energy and water sectors. Scenarios depicting how the regions' infrastructure are connected and how they were subsequently impacted by the various injects were captured in PowerPoint presentations and videos, which were then utilized in the exercises.

H.1. Charleston Exercise Findings

INL supported the energy sector table for the Charleston exercise by supplementing the discussion with pointed questions to the owners and operators from the energy sector. The intent was to facilitate a dialogue to identify how the various stakeholders would respond to the situations presented within each turn. The players from the energy sector did not seem to believe the injects would have a debilitating impact on their operations. This could have been rectified through interacting more with the stakeholders prior to the workshop as well as focusing on the bulk transmission of energy versus the distribution aspects.

The injects in which the electricity substation was compromised resulted in some discussion during the Charleston exercise; however, utility participants thought they would be able to work around the issue. INL believes this was due to a lack of clarity in the scale of the event and language used. If AHA results were shown, INL believes participants' responses would have been altered. It was not clear from the discussion how Dominion Energy tests firmware configuration changes. Notes of interest included:

- On multiple occasions, a utility participant expressed that someone else within their organization would be responsible for determining whether they were experiencing a cyberattack.
- The Charleston energy table participants never reached the conclusion they were under attack. As stated below, the advisory/alert and phishing threads played almost no role in the discussion.
- The virtual environment resulted in some challenges getting injects out of DECIDE® and inserted into the discussion. As a result, the moderator summarized each inject at the being of each turn.
- Some discussion occurred on the segregation of control and business networks—specifically, which computers were impacted. Participants believed the computer-based injects implied business system computers (i.e., IT, not OT).
- Local workarounds discussed included disconnecting control devices and operating in manual mode.
- Participants did not have concerns about being able to access the substation.

H.2. Savannah Exercise Findings

INL supported the energy table in the Savannah exercise by supplementing the discussion with pointed questions to the owners and operators from the energy sector. The intent was to facilitate dialogue to identify how the various stakeholders would respond to the situations presented within each turn. The JV instance of AHA was leveraged during the exercise to help participants visualize the infrastructure being discussed during each turn. This seemed to assist with getting the injects to resonate with the participants and teasing out additional context that likely would not have otherwise been discussed.

The inject involving a compromise of natural gas compressor station firmware resulted in significant discussion during the Savannah exercise. The Savannah participants had a mix of cybersecurity and engineering representatives who were able to piece the scenario together. In addition, showing results from AHA resulted in a quick realization that this was a significant event and would result in significant interruptions in service. The cybersecurity representatives quickly picked up on the scene setter injects, which resulted in in-depth gameplay discussions. However, some participants were confused by language used in the inject to describe the events taking place. Notes of interest included:

- Cybersecurity personnel were actively engaged and cyber compromise was rapidly considered.
- Local workarounds including disconnecting control devices and operating in manual mode.
- Participants had no concerns about being able to access the substation. Participants discussed potentially involving company security personnel in the response.

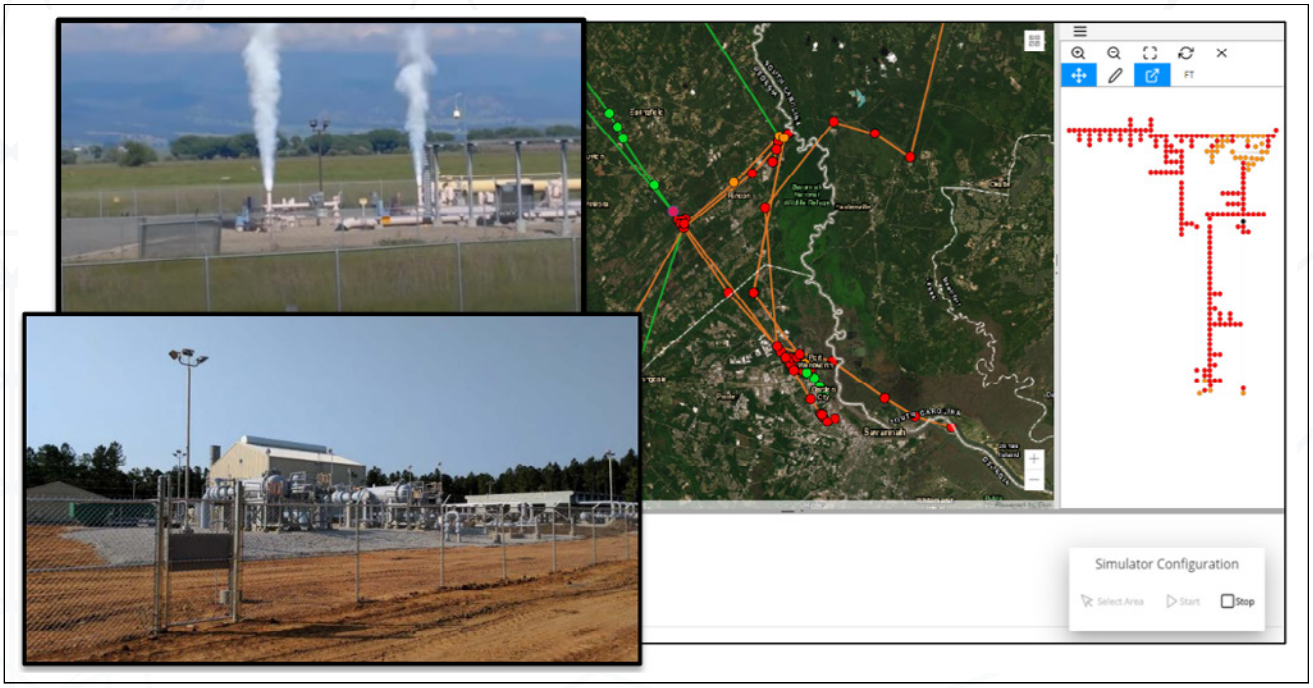


Figure 26: Excerpt from Turn 5 PowerPoint Slide—Natural Gas Compressor Stations

H.3. Lessons Learned

Inject planning: INL supported the development of the injects utilized throughout the turns of the JV exercises. By the time the INL team was brought in to support this area, the inject planning was in progress and the development of the Master Scenario Event List (MSEL) was already underway. If the AHA simulation had been involved from the initial stages of planning, the turns and injects could have allowed for a more robust scenario. Analysis of downstream infrastructure and the associated impacts in the event operations became degraded would identify potential assets that may not have been identified in the JV 3.0 exercises.

Obfuscation of infrastructure names: Throughout the process of developing the infrastructure to be included in the scenario, the INL team obfuscated the names of the assets in the JV instance of AHA. This was performed under the assumption the exercise needed to be agnostic regarding the actual infrastructure within the Charleston and Savannah regions. As the exercise played out, it became clear the scenario resonated more with the stakeholders when the actual infrastructure names were used in describing where the events of the scenario were occurring.

Interaction with service providers: The primary interaction the INL team had with the service providers involved in the exercise was during the exercise itself. The dialogue with the service providers uncovered nuances about their operations that would have been beneficial to know during inject planning. A brief interaction occurred during the rehearsal sessions, but that discussion was mainly focused on the water sector. During the actual exercise, INL supported the energy table and did not have any direct interaction with the water sector.

Earlier engagement with service providers would allow for better understanding of the presence—or lack thereof—of alternate sources of critical products required for operations. This bottom-up level of detail would allow for more tailored scenario planning that could reveal supply chain issues that may only arise when alternate modes of operations are being leveraged.

Use of terminology and focus areas: The primary focus of the impacts on the energy sector during the scenario was on the infrastructure involved with the distribution of the commodity (i.e., distribution substations or distribution pipelines). Impacts on these infrastructure resonate with the downstream asset owners who are depending on the commodity being provided, but the service providers were generally able to rectify the consequences of impacts at this level fairly quickly by either switching to manual operations or redirecting the load to a different set of distribution infrastructure. If the focus area of the impacts were to be shifted to the bulk transport of commodities (i.e., transmission substations or compressor stations), the impacts would be on a broader scale, but the response by the service providers to control the impact would not be as easily identifiable. Consideration should be given to transmission infrastructure in planning future injects and scenarios.

APPENDIX I – CIRI FORT-TO-PORT DISRUPTION

Introduction

A primary objective of the JV 3.0 exercises was to understand the impact of cyber-originating disruptions on power projection. To address this objective, this appendix focuses on interactions between communications/IT systems and their impact on the Maritime Transportation System (MTS). Specifically, the report uses data sources—publicly available geographic information system (GIS) data and movement schedules provided by SDDC—to quantify the impact of cyber-originating disruptions based on known historical incidents. The incidents considered are consistent with the JV 3.0 injects, which took a gray-zone approach. The baseline behavior as well as the impact of a disruption as computed by a multicommodity network flow optimization algorithm (an extension of work by Boland et al.) was validated by interactions with stakeholders at SDDC and others.[49]

The fort-to-port analyses developed for these exercises extend the Port Disruptions Tool (PDT)—developed by the Critical Infrastructure Resilience Institute (CIRI)—to quantify the impact of such disruptions. Beyond the practical impact on understanding power projection, CIRI believes such analyses extend the current state of the art reflected in datasets such as Harmonized Grids of Critical Infrastructures in Europe (commonly known as "HARCI-EU"), a grid-based approach to critical infrastructure risk assessment.[50]

Given the increased dependence on communications/IT systems because of the pandemic, the widespread intrusion of nation-state actors into U.S. critical infrastructure systems, and civil unrest targeting such systems, the ability to model and prepare for such events is an increasingly essential capability for both government and private industry.[51]

[49] Natashia Boland et al., "The Continuous-Time Service Network Design Problem," *Operations Research* 65, issue 5 (September-October 2017): 1111–48.

[50] Filipe Batista e Silva et al., "HARCI-EU, a Harmonized Gridded Dataset of Critical Infrastructures in Europe for Large-Scale Risk *Assessments," Scientific Data*, 6, no. 126 (2019).

[51] Natasha Veligura et al., *The Impact of COVID-19 on the Global Telecommunications Industry* (Washington, DC: International Finance Corporation, updated May 2020); Hannah Murphy and Demetri Sevastopulo, "US Says Cyber Hack Poses 'Grave Risk' to Critical Infrastructure," *Financial Times*, December 17, 2020, https://www.ft.com/content/edbad243-28ed-4133-98a0-1447a7213abf; and Shane Harris, "Nashville Bombing Is a Potent Reminder That Communications Systems Remain at Risk from Attack," *Washington Post*, December 28, 2020, https://www.washingtonpost.com/national-security/nashville-bombing-is-a-potent-reminder-that-communications-systems-remain-at-risk-from-attack/2020/12/28/d734b76c-4949-11eb-839a-cf4ba7b7c48c_story.html.

Data Sources

The table below illustrates the data sources used in the analysis.

Data Sources						
Sector	**Layer**	**Type**	**Source**	**Format**	**Resolution**	**ID**
Transportation	Road	Network	USGS National Transportation Map	.shp	Nation	DS-TR.N-1
			Charleston roadways	.json	City, port	DS-TR.N-2
		Flows	SDDC truck movements	.ppt	Region	DS-TR.F-1
			SDDC roadway flows	.json	Region	DS-TR.F-2
	Railway	Network	USGS National Transportation Map	.shp	Nation	DS-TR.N-3
			SC railways	.json	State	DS-TR.N-4
			Federal Railroad Administration, rail junctions	.shp	Nation	DS-TR.N-5
		Flows	SDDC rail movements	.ppt	Region	DS-TR.F-3
			SDDC railway flows	.json	Region	DS-TR.F-4
Communications/ IT	Fiber	Network	Source not found	n/a	Region	DS-CM.N-1
			Source not found	n/a	City, port	DS-CM.N-2
	Cellular	Network	DHS HIFLD cell towers	.shp	Region	DS-CM.N-3
			SC cell towers	.json	State	DS-CM.N-4
	Cross-Layer	Network	Comms-transportation exercise injects	.xls	Region	DS-CM.N-5
			Comms-transportation dependencies	.json	City, port	DS-CM.N-6

Table 8: JV 3.0 Data Sources

Critical Infrastructure Networks

At a high level, CIRI has created a multilayered network whose layers correspond to critical infrastructure networks. This study focuses on interactions between the communications/IT sectors and their impact on the transportation sector. If desired, future work could integrate dependencies on the electrical power system, building on expertise gained via the Defense Advanced Research Projects

Agency Rapid Attack Detection, Isolation and Characterization Systems at the University of Illinois at Urbana-Champaign (UIUC).[52]

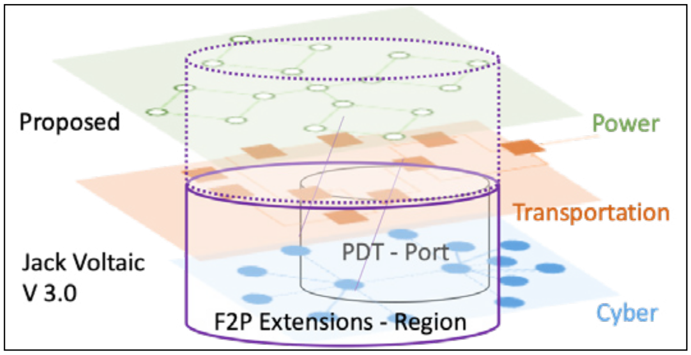


Figure 27: A Multilayered Network Model for Critical Infrastructure

Transportation Sector: Intermodal transportation networks were directly extracted from the GIS data sources listed above. These GIS files were processed, via the NetworkX package from Los Alamos National Laboratory, into directed networks that use the L-space representation.[53] In the L-space representation for transportation networks, vertices within a network correspond to locations, edges correspond to roadways/railways, etc.[54] The SC railway network (DS-TR.N-4) resulting from the GIS file (DS-TR.N-3) has 2,732 nodes; this is similar in size to 2,500, the average number of nodes in railway networks provided by a 2013 survey of L-space representations for transportation networks.[55] To optimize commodity flows across such a network, however, CIRI needed to reduce the size of the network. For example, the paper by Boland et al. in the transportation network optimization literature considered benchmarks for fixed graphs that were 20–30 nodes, 230–700 arcs, and 40–100 commodities.[56] Therefore, we employed various approaches to reduce the size of the transportation network graphs. The approach we adopted, based on a paper by Buchsbaum and Westbrook, constructs a hierarchy tree to adaptively collapse groups of transportation network locations into a single node according to their geographic proximity to one another.[57] Depending upon the degree of resolution desired for an analysis, different levels of detail in the network are preserved (including properties such as travel time and cost through a subgraph). More details about this approach can be provided by CIRI on request. Note that once this transformation occurs, the networks no longer may be considered as using an L-space representation.

Cyber Disruptions with Secondary Impacts on Power Projection

This section provides an overview of three types of cyber-originating disruptions to power projection based on real-world incidents:

1. Train derailment due to compromised rail-control signals
2. Rail delays due to communications network degradation
3. Traffic congestion resulting from cyberattacks

[52] Walter Weiss, "Rapid Attack Detection, Isolation and Characterization Systems (RADICS)," Defense Advanced Research Projects Agency (website), n.d., https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems, accessed January 5, 2021.

[53] Aric A. Hagberg, Daniel A. Schult, and Pieter J. Swart, "Exploring Network Structure, Dynamics, and Function Using NetworkX," in *Proceedings of the 7th Python in Science Conference (SciPy 2008)* (self-pub., 2008), http://conference.scipy.org/proceedings/scipy2008/SciPy2008_proceedings.pdf.

[54] Julian Sienkiewicz and Janusz A. Hołyst, "Statistical Analysis of 22 Public Transport Networks in Poland," *Physical Review E* 72, issue 4, part 2 (October 2005).

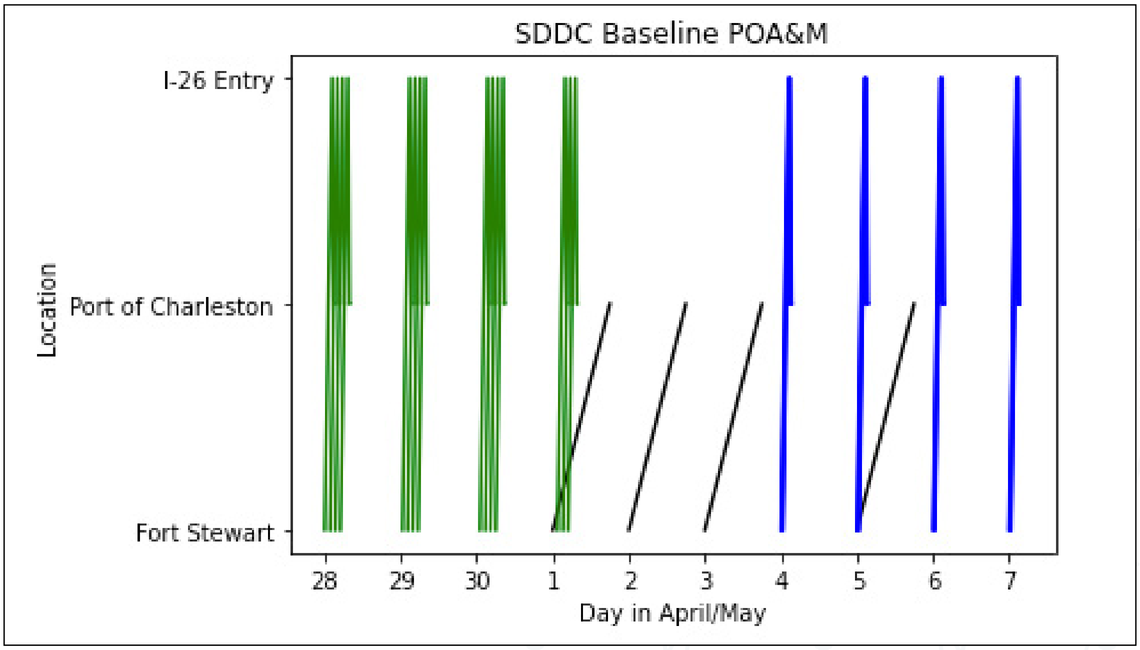
[55] Jingyi Lin and Yifang Ban, "Complex Network Topology of Transportation Systems," Transport Reviews 33, issue 6 (2013).

[56] Boland et al., "Continuous-Time Service Network Design Problem," 1111–48.

[57] Adam L. Buchsbaum and Jefferey R. Westbrook, "Maintaining Hierarchical Graph Views," in *SODA '00: Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms* (Philadelphia: Society for Industrial and Applied Mathematics, February 2000), 566–75.

Baseline Context

The context for discussion of these disruptions is the SDDC Baseline Plan of Action and Milestones that was provided as part of the JV 3.0 exercises. The time-location diagram in figure 28 plots intermodal road and rail movements from Fort Stewart to the North Charleston Terminal used by the 841st Transportation Battalion command. Commercial line haul, convoy, and train movements over the course of the exercise time line are shown. The accompanying table presents the dates used to instantiate the diagram. Times from source to destination along optimal routes were calibrated via a combination of feedback from SDDC and Google Maps, as discussed in more detail below.



Type	Start	End	Notes
Rail Upload	May 1	May 5	Instantiated on May 1, 3
Rail Download	May 1	May 7	Instantiated on May 2, 5
Convoys	May 4	May 7	5 serials a day, 4 days
Line Haul	April 28	May 1	150 trucks over 4 days

Figure 28: Intermodal Road and Rail Movements from Fort Stewart to North Charleston Terminal Used by the 841st Transportation Battalion Command.

Disruption 1 (D1): Derailment via Infrared Hack

In the JV 3.0 exercise, the MSEL included an inject on Tuesday morning during which “Norfolk Southern notified SDDC that a major rail line servicing Fort Stewart to the Port of Charleston was taken offline to investigate malfunctions in a switching station.”

One possible cause of switching station malfunctions includes spoofing or jamming switching the control signals. Such an incident occurred in a Polish tram hacking attack in 2008. On this occasion, a 14-year-old boy used a homemade infrared transmitter to trip rail switches and redirect trains. Four trams were derailed, and a dozen people injured.[58] The device, made from a television controller, was capable of controlling all junctions on the line, and the boy had written in his schoolbook where the best junctions for moving trains around were.[59]

After consulting with SDDC, the team learned that most rail switches in the contiguous United States are controlled by line of sight. Although the rail companies have a smart system for checking the rail via a networked service, track switching depends on radio signals sent from the engine to the switch. Rather than derailment via infrared signal hacking, a replay attack could be employed to spoof a signal and switch the track. Alternatively, a jammed radio signal could cause derailment because a train may need to adjust its speed when traversing a junction. Beyond rail delays, a secondary impact of a derailment on the communications network could be a severed fiber cable because fiber is also placed along rail rights-of-way.

Data Sources and Calibration: To model such a disruption, the CIRI team constructed a rail transportation network based upon publicly available GIS data from the United States Geological Survey (USGS) National Transportation Map (DS-TR.N-3) as well as the Federal Railroad Administration's rail junctions (DS-TR.N-5). Vehicle schedules provided by SDDC were used to determine when trains left Fort Stewart and when they were expected to arrive at the Port of Charleston. The CIRI/ACI team consulted with SDDC to calibrate the baseline routes computed, the duration of the train route (18 hours), and the speed of the train. The duration of the train on the route, as noted during the discussion, does not include staging, prepping, and loading of material onto the train. Other factors that may affect train speed include tunnels, bridge limitations, terrain, and environment (e.g., flooding); these were not modeled.

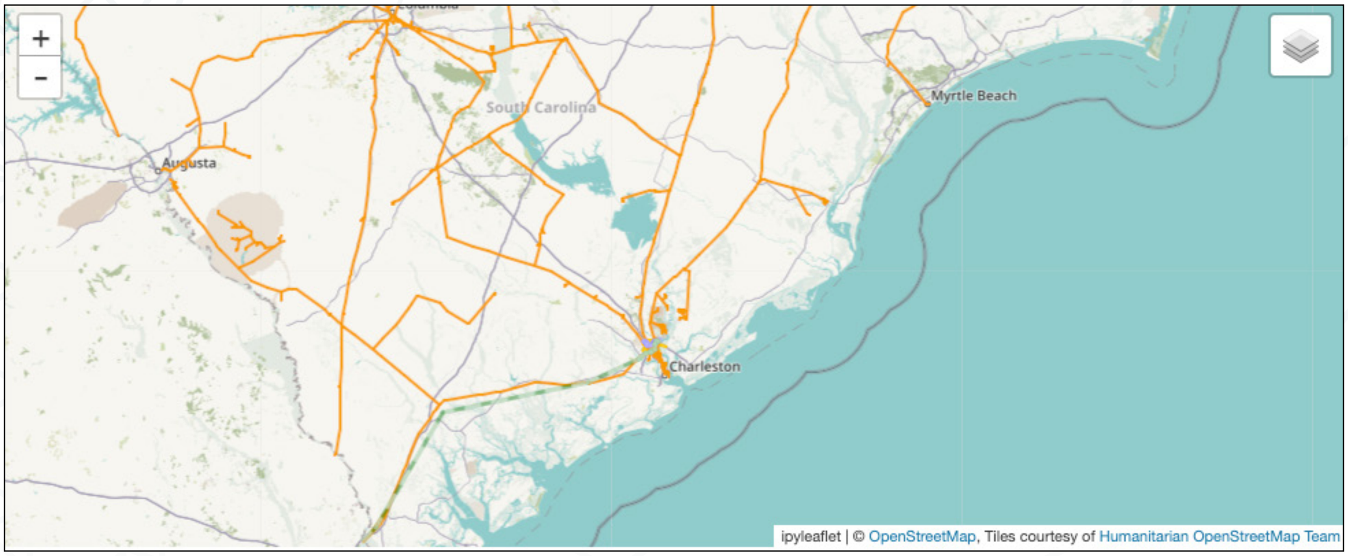
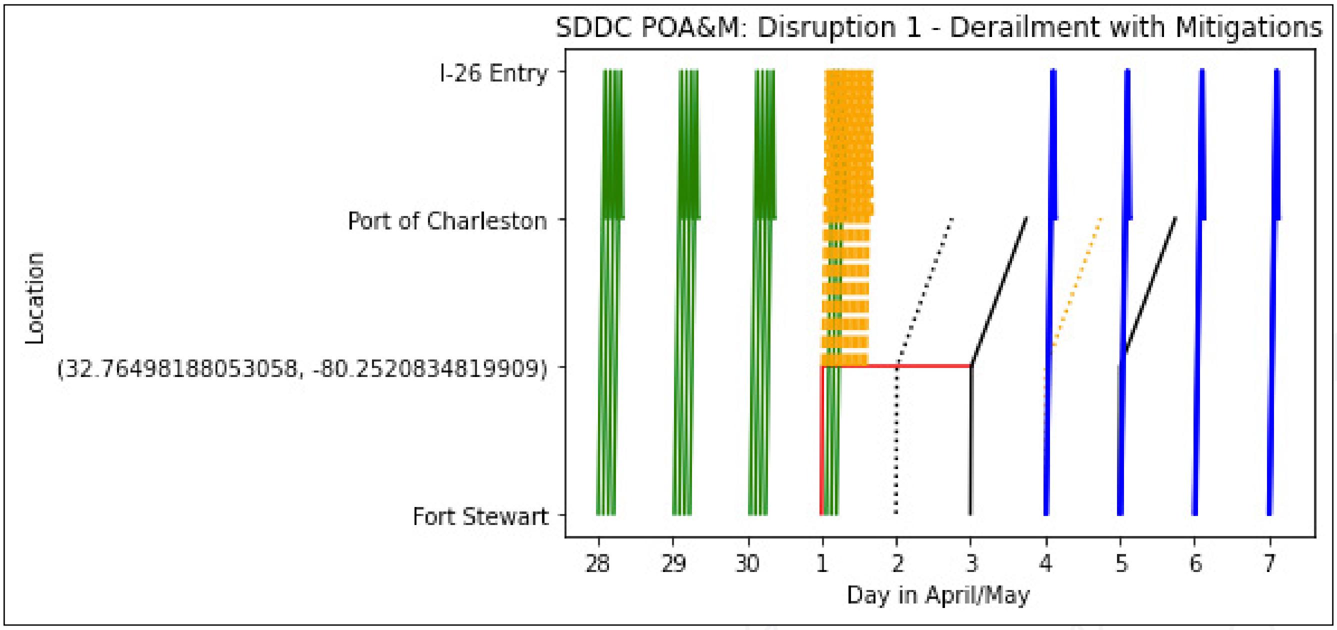

+
-
Columbia
South Carolina
Myrtle Beach
Augusta
Charleston
ipyleaflet | © OpenStreetMap, Tiles courtesy of Humanitarian OpenStreetMap Team

Figure 29: Baseline rail movements from Fort Stewart to Charleston (shown in green) along a regional rail network provided by USGS (shown in orange).

[58] Chuck Squatriglia, "Polish Teen Hacks His City's Trams, Chaos Ensues," Wired, January 11, 2008, https://www.wired.com/2008/01/polish-teen-hac/.

[59] Tim Wilson, "Teenage Hacker Takes Over Polish Tram System," Dark Reading, January 11, 2008, https://w2.darkreading.com/attacks-breaches/teenage-hacker-takes-over-polish-tram-system/d/d-id/1129231?&.

Figure 29 illustrates the regional rail network provided by the USGS National Transportation Map (shown in orange). One key takeaway is that in the case of the Port of Charleston, there appears to be one direct route from Fort Stewart to the Port of Charleston (shown in green). This could lead to a single point of rail failure. A second route through Columbia, though less direct, provides a potential alternative route. The impact of a derailment on the SDDC Plan of Action and Milestones is illustrated in figure 30.



Type	Start	End	Notes
Rail upload	May 1	May 5	May 1 train derailed.
Rail download	May 1	May 7	May 2 train disrupted.
Convoys	May 4	May 7	5 serials a day, 4 days
Line haul	April 28	May 1	150 trucks over 4 days
Mitigation and response	May 1	May 2	45 trucks with departures every 30 minutes starting 0.5 days after derailment. May 2 train rescheduled.

Figure 30: Impact of a Derailment on the SDDC Plan of Action and Milestones

The derailment CIRI modeled occurs shortly after the junction at Yemassee, where the line from Fort Stewart branches between Charleston and Columbia, SC. Note that to get the pieces from the derailed May 1 train, line haul trucks (shown in orange) are sent from the point of disruption (just after the railway splits in Yemassee) to the North Charleston Terminal. Based on fieldwork with Port Everglades and the Florida East Coast Railway, CIRI estimated a derailment would take 2 days to clear. As a result, the train on May 2 (shown in dashed black lines) as well as possibly May 3 (not shown) are affected. There may be three options to address this delay: wait to move the train until the derailment has been cleared; use another mode of transportation to the port; or, if possible, reroute the trains scheduled to depart around the obstructed railway.

The first case in the time-location diagram illustrates that it may be possible to reschedule the May 2 train to May 3 or 4 (shown in dashed orange). In the case of May 3, the rescheduled train might interfere with the train originally scheduled for May 3, but this would cause less delay at the port if the order of arrival of pieces were significant. In the case of May 4, other alternative modes of transport could be useful. There may be a risk associated with reducing the slack between shipments on rail.

The second response option would have the fort move pieces originally scheduled for the May 2 train via commercial long haul. It would be important to consider the risks of increased gate utilization to determine the impact of a gate outage (e.g., gate operating system [GOS] failure). Queueing theory provides a formalism for exploring such considerations and is part of the PDT discrete-event simulation tool. In addition, increased dependencies on trucking companies could increase the impact of disrupting such a company's telemetry network.

A third option, if the derailment allowed it, would be to reroute the scheduled trains. This might make sense if the time frame or risk associated with the option were more optimal than the time frame or risk associated with the first and second options. SDDC stated that such an option would likely not be chosen. Nonetheless, this analysis considers the cyber-physical risks of rerouting a train.

According to SDDC, this alternative route is determined by the rail company (Norfolk Southern). The PDT multicommodity network flow optimizer selected a route through Columbia to explore secondary effects on transportation and communications systems as goods move via this alternative route (shown in figure 31).

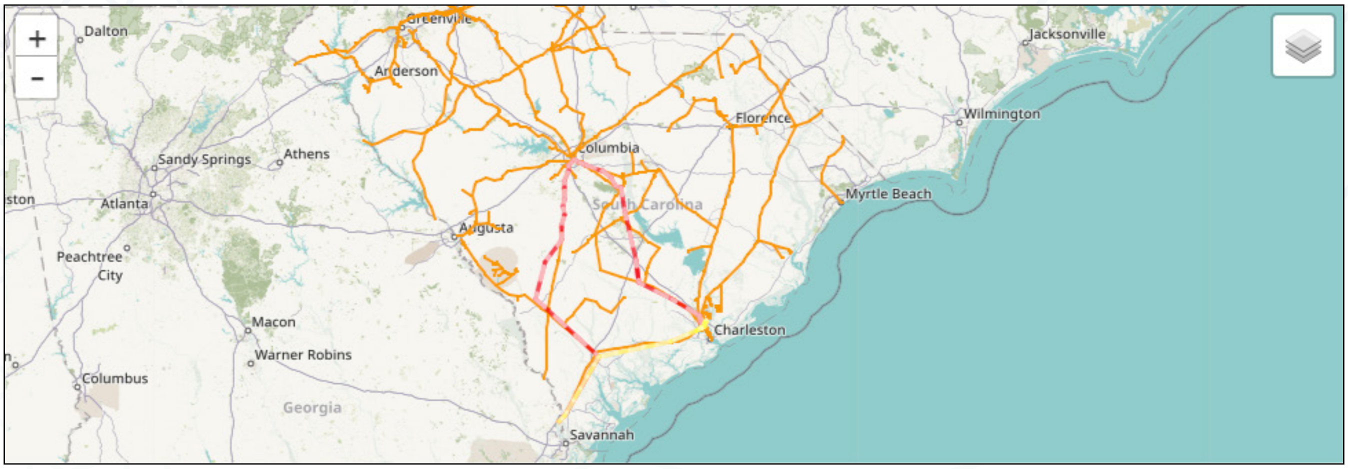


Figure 31: A derailment close to the junction at Yemassee would force a delay and possibly reroute the train. Regional routes are shown for a derailment whose impact lasts from April 26–28 (day 3). Alternate routes (shown in red) are for trains 2 and 3.

Rerouting vehicle movements has secondary effects on social, local transportation, and communications domains. First, from a social standpoint, JV 3.0 chat logs suggest that rerouting movements would require a battalion commander to request support from a higher command: “841st Battalion: Roadblock requires support from higher command, battalion commander will submit a written doc to command requesting support to look at diverting assets from brigade to request follow on actions. Engage with Base and Port Readiness Committee.” Second, local transportation systems in Charleston (or even Columbia) may be affected if pieces are rerouted via vehicle or train. Figure 32 illustrates a local view of train routes taken through Charleston under normal (yellow) and disrupted (red) conditions. The section on Disruption 3 (D3) later in this appendix demonstrates how the choice of route may affect the ability of an adversary to further disrupt movements. Third, the impact of rerouting vehicle movements on the communication domain is the focus of the next section, “Disruption 2 (D2).”

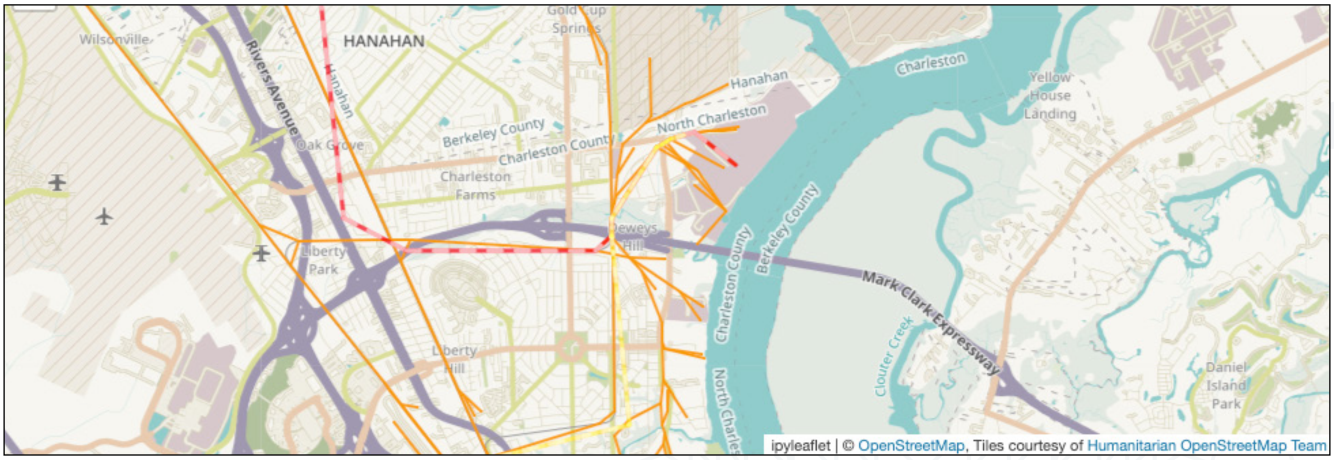


Figure 32: Rerouting movements in a rural location can impact local movements through the city. Baseline and disrupted transportation flows (yellow and red, respectively) are illustrated here.

Key Takeaways:

- There is one primary rail route from Fort Stewart to Charleston.
- Jamming or spoofing of rail signals can result in derailment.
- According to SDDC, a derailment in the city would be worse than in a rural area.
- But rerouting from a rural area (either by rail or road) can still affect city transportation movements and cause delays in train arrivals to the port.
- The choice of route is up to the rail company (private industry), but it must be approved by higher command.

Disruption 2 (D2): Rail Delays Due to Communications Network Degradation

Railroad companies are increasingly adopting digital communications as a cheaper and more easily maintained technology than copper. For example, Norfolk Southern “uses cell phones to transmit data between field sites and central offices.”[60] CSX Transportation has conductors and field workers

[60] Angela Cotey, “Railroad Communications Technology: From Cellular to Radio to Satellite to Wi-Fi,” Progressive Railroading, May 2012, https://www.progressiverailroading.com/norfolk_southern/article/Railroad-communications-technology-from-cellular-to-radio-to-satellite-to-Wi-Fi--30947.

communicate with each other through cell phones, including applications on the phones. These applications include reporting systems for conductors, services for track inspectors and signal maintainers, and applications for communications with truck drivers and intermodal yard operators. Wi-Fi is also used for communications in remote locations, with railroad companies building their own networks to cover regions with no cell coverage.

During the JV 3.0 exercises, some injects might have been caused by disruptions to a railroads' communications networks. For example, on Monday at 6:01 p.m., county transportation officials discovered a wireless router connected to a traffic box in a remote location. Such routers could also have been deployed in a remote region of a railroad's wireless network and thereby affected communications. In addition, on Tuesday at 3:47 p.m., Norfolk Southern had its crews verify that rail lines were clear and had not been tampered with or damaged. However, communications required to use the rail could have been damaged.

In an alternative scenario, however, communications required for using the rail could have been damaged. During discussion of the scenario with SDDC, it was observed that if a cell tower were to go down, other towers in the area could pick up service, and even if a signal were lost, it would be just an annoyance. However, during the exercise, stakeholders often commented on their concern over communications going down. In addition, degradation of the cell phone network could result in loss of data upon which many of the previously mentioned digital communications adopted by railroad companies depend.

An additional concern is man-in-the-middle (MITM) attacks via unmanned aerial vehicles (UAVs). Specifically, UAVs could provide a Wi-Fi signal that could be used to steal signals from a rail company's rural wireless networks. UAVs are used to patrol by railroads because rail police cannot access remote locations. Thus, such a capability could be used by an adversary. SDDC confirmed that whether the rail route is covered by satellite, cell, or Wi-Fi, such a threat model is worth exploring further.

Data Sources and Calibration: In addition to the aforementioned data sources provided by USGS, this analysis uses the Department of Homeland Security (DHS) Homeland Infrastructure Foundation-Level Data's (HIFLD's) GIS data on cell phone tower locations (DS-CM.N-3). These locations were used to compute a Voronoi diagram to determine which cell phone towers provided which communications along the railway network.

Figure 33 illustrates the cell phone tower coverage along several rail routes from Fort Stewart to Charleston's North Terminal. The interaction between the choice of route taken and communications networks should be considered to protect potentially sensitive information about movements.

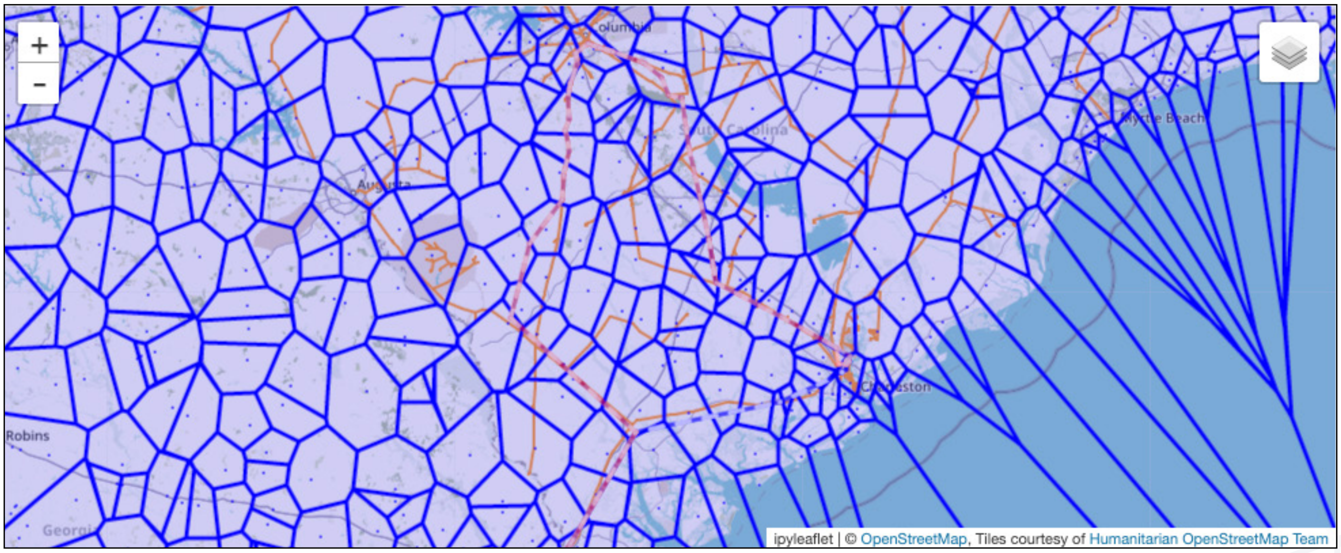

+
-
olumbia
South Carolina
Myrtle Beach
Augusta
Charleston
Robins
Georgia
ipyleaflet | © OpenStreetMap, Tiles courtesy of Humanitarian OpenStreetMap Team

Figure 33: This figure depicts coverage provided by cell phone towers modeled as a Voronoi diagram. The points within each blue region connect to the same (closest) tower. Choice of route taken by rail should also consider the communications networks upon which movements depend.

For example, changing the route in response to a derailment, as in Disruption 1, affects the cell phone towers (and potentially companies) upon which power projection depends. This is shown in more detail for Charleston in figure 34.

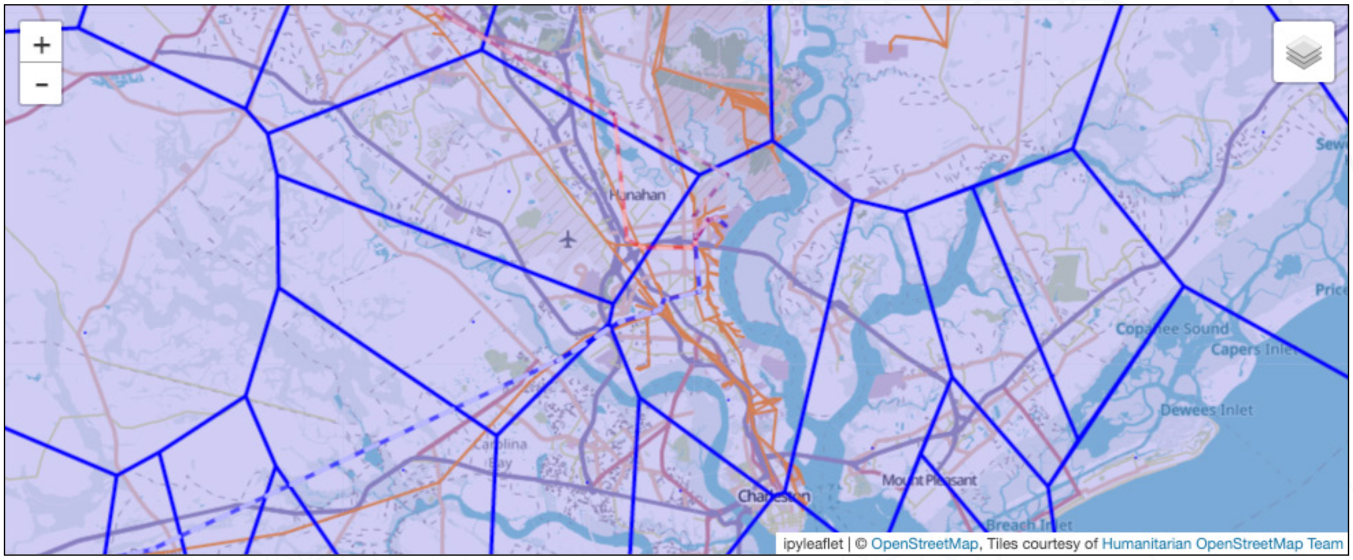


Figure 34: Choice of route taken by rail should also consider the communications networks (and companies) upon which movements depend.

Key Takeaways:

- Route choice may affect the exposure of data to adversaries, depending upon the communications networks utilized.
- Exposure to UAV-based MITM attacks may be worse in rural areas, where railroad companies rely on wireless networks.
- Technologies such as Stingray may also enable one to use MITM methods to access operational data via cell phone signals used by emerging applications employed by rail companies.

Disruption 3 (D3): Traffic Congestion Resulting from Cyberattacks

In addition to potentially altering a movement's risk posture in the cyber domain, rerouting vehicle movements in response to an initial disruption may also increase risk relative to other domains. For example, by diverting rail movements through the more heavily populated area of a municipality (e.g., due to the rural disruption in D1), protestors may have more chances to disrupt the route once the train enters the city. An example of such an occurrence is the cyberattacks and reinforced protests that affect the Bay Area Rapid Transit system. Similar disruptions might be possible during power projection through a city.

During the JV 3.0 exercises, several MSEL injects involved protestors blocking or otherwise affecting traffic. For example, on Monday morning, the main access gate sporadically failed to open, and on Tuesday afternoon, main terminal gates were the site of protests. A failed GOS can cause significant traffic congestion at a port. For example, the NotPetya ransomware affected one Maersk terminal where trucks collected "bumper to bumper, farther than [one] could see."[61] The PDT has been used to model the impact of GOS outages.[62] This scenario considers the impact of protests causing the rerouting of rail and vehicle movements through a common cell phone tower.

In addition, exercise chat logs reflect related concerns by exercise participants. First, stakeholders were concerned about congestion on roadways, especially when combined with rail line degradation: "SDDC concerned about crash on I95 (other Feds not aware) and impact on degrading Ft. Stewart movement; especially in light of rail line degradation." Furthermore, congestion resulting from protests can degrade the ability to keep military and commercial traffic separate: "841st wondering how the protests and gate issues would affect one's ability to keep military and commercial traffic separate. They could manually validate TWIC but a military truck could go in the commercial side of the port."

Data Sources and Calibration: The same datasets as those mentioned previously were used in this analysis. In addition, vehicle movements by roadway were obtained from SDDC that were aligned with the JV 3.0 scenario time line. The choice of roadway routes was validated using Google Maps for traveling from I-26 in the northwest corner of the city to North Charleston Terminal. Note that the primary and secondary road optimal routes computed by the PDT optimizer align with the routes chosen by Google Maps for the same source and destination. The computed optimal routes approximately follow the GIS roadways because they were computed on GIS transportation networks

[61] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[62] Gabriel A. Weaver, Mark Van Moer, and Glen R. Salo, "Stakeholder-Centric Analyses of Simulated Shipping Port Disruptions," in 2019 Simulation Winter Conference (New York City: Institute of Electrical and Electronics Engineers, 2019).

reduced in size via the aforementioned method based on hierarchy trees.[63] Vehicles moved on the roadway at 55 miles per hour and were considered late if they arrived after more than 30 minutes (Google Maps estimated that the trip would take 9 minutes).

Figure 35 illustrates baseline road and rail routes through Charleston (shown in green and blue, respectively) as well as rerouted rail routes in response to D1 (shown in red). As a result of this response to D1, there appears to be a potential single point of disruption along the Mark Clark Expressway where road movements are affected. Moreover, this point of convergence within a small geographic region opens up opportunities for communications network disruptions or data gathering, as discussed in D2.

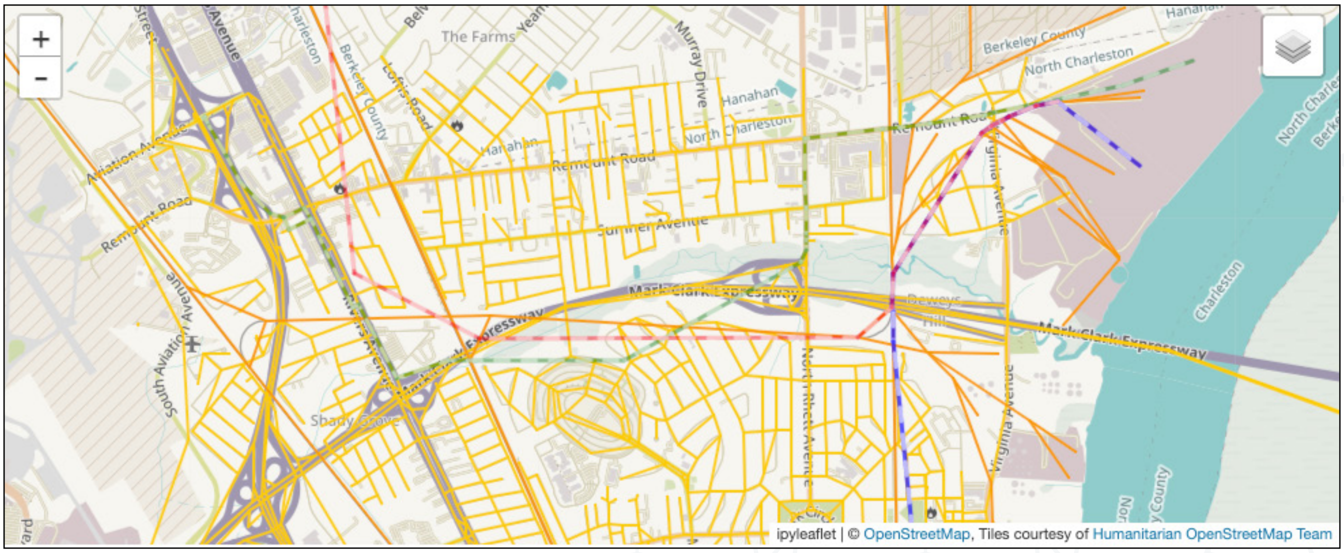


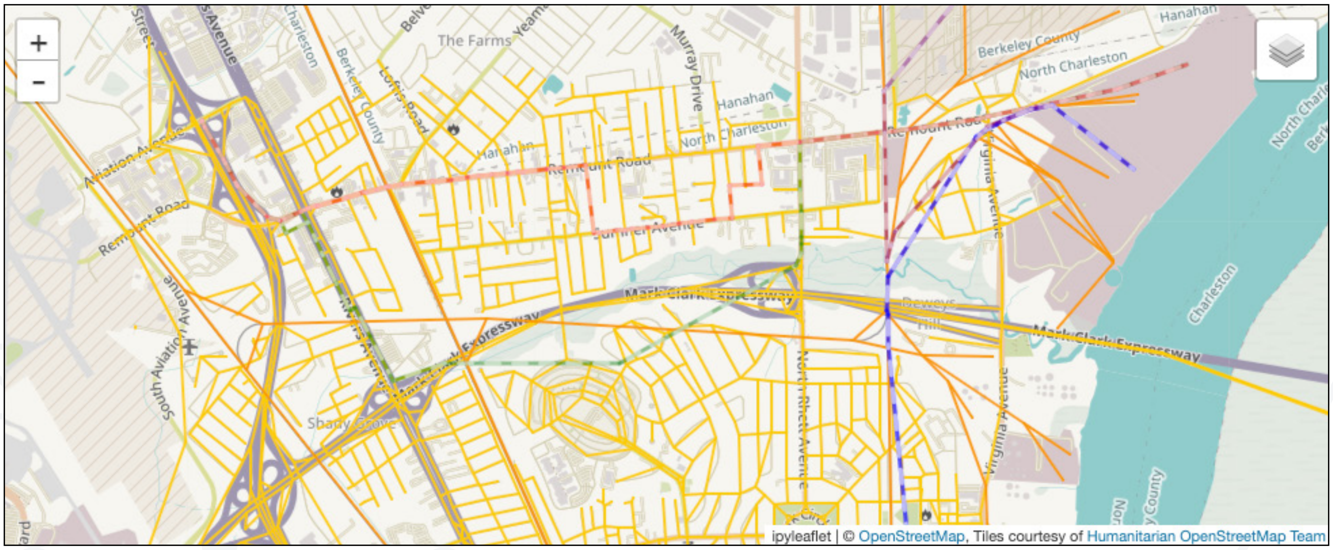
Figure 35: Baseline road routes through Charleston shown alongside baseline and disrupted rail routes (blue and red) following derailment in D1.

CIRI modeled a 1-day protest. This protest would directly affect commercial line haul, which travels from fort to port if held sometime during April 27–30. In the context of train derailment mitigation actions (D1), a protest held on May 1 could interfere with additional line haul traffic carrying pieces from the derailed train. In the context of response actions to transport pieces from the May 2 train, a protest on May 2–4 could interfere with either commercial long-haul trucks carrying rescheduled pieces or rerouted trains moving via Columbia.

Specifically, if the protestors were able to simultaneously disrupt the nearby rail line taken by rerouted trains, another mitigation would have to be considered for rail as well. We note that, alternatively, unrelated protests might also occur in Columbia (as described in D1) to disrupt rail movement but have less effect on long-haul and convoy routes.

[63] Buchsbaum and Westbrook, “Hierarchical Graph Views.”

Figure 36 illustrates the recomputed optimal road and rail routes (shown in red and purple, respectively), given a hybrid disruption consisting of a rural train derailment and city protestors demonstrating along the highway. We note that this shifts the intersection of rail, traffic, and cell phone towers to a new, single geographic region at the intersection of Remount Road and Virginia Avenue.



ipyleaflet | © OpenStreetMap, Tiles courtesy of Humanitarian OpenStreetMap Team

Figure 36: Rerouting road and rail movements in response to a protest on Mark Clark Expressway results in a new potential disruption point at the intersection of Remount Road and Virginia Avenue.

Key Takeaways:

- Rerouting traffic can result in new single points of failure across multiple critical infrastructure domains.
- Planners should be aware of changing risk due to the data or stakeholder dependencies of secondary and tertiary routes and time delays resulting from disrupted movements.

Broader Impact

The scenarios considered in this appendix are based on historical incidents in which MTS stakeholders were disrupted via their communications/IT systems. The function of the MTS depends upon cross-organizational coordination among multiple stakeholder organizations. Cyber-originating disruptions experienced by these stakeholders, such as those listed in table 9, might be leveraged by an adversary during coordinated gray-zone disruptions like those exercised during JV 3.0.[64] Some Port of Charleston stakeholders opined that this level of dependence creates a requirement for information sharing and analysis organizations focused on the needs of specific regions.

In table 9, each incident is grouped by the type of stakeholder that was affected; the corresponding affected systems and Common Attack Pattern Enumeration and Classification identifiers (CAPEC-IDs) are also listed.[65]

Historical Communication/IT System Incidents among MTS Stakeholders

Stakeholder	Attestation	System	CAPEC-ID
Shipper	BW Group	Unknown	CAPEC: Subvert Access Control
	A.P. Mollar Maersk	Accounting software	CAPEC 549: Ransomware
	USTRANSCOM Contractor	Multiple systems	Unknown
	Black Sea	GNSS/GPS	CAPEC 616: Spoofing
Law enforcement	DC Police	Surveillance camera (RDP)	CAPEC 629: Surveillance Camera Compromise
	WI Law Enforcement	Comms/email	CAPEC 549: Ransomware
Trucking company	USTRANSCOM Contractor	Email	CAPEC 163: Spear Phishing
	Unknown	Electronic logging device (ELD)	CAPEC 629: Unauthorized Use of Device
	Unknown	Wi-Fi	CAPEC 157: Sniffing
	Unknown	USB	CAPEC 523: Timer-Activated Malware

[64] Greenberg, "The Untold Story"; Sameer C. Mohindru, "Shipping: BW Group's Computer Systems Hacked; Steps Up Cyber Security," S&P Global Platts, October 2017, https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/101317-shipping-bw-groups-computer-systems-hacked-steps-up-cyber-security; Marvin the Robot, "New Petya / NotPetya / ExPetr Ransomware Outbreak," Kaspersky Daily (blog), June 27, 2017, https://usa.kaspersky.com/blog/new-ransomware-epidemics/11710/; Senate Committee on Armed Services, *Inquiry into Cyber Intrusions Affecting U.S. Transportation Command Contractors* (Washington, DC: U.S. Government Printing Office, 2014); Miranda Green, "Romanian Hackers Infiltrated 65% of DC's Outdoor Surveillance Cameras," CNN, December 20, 2017, https://www.cnn.com/2017/12/20/politics/romanian-hackers-dc-cameras/index.html; Division of Emergency Management, 2016 State of Wisconsin Hazard Mitigation Plan (Madison, WI: Wisconsin Department of Military Affairs, December 2016); Burney Simpson, "Cyberattacks Called a Growing Threat to Trucking Industry," Transport Topics, June 7, 2018, https://www.ttnews.com/articles/cyberattacks-called-growing-threat-trucking-industry; Tom Bateman, "Police Warning after Drug Traffickers' Cyber-Attack," BBC News, October 16, 2013, https://www.bbc.com/news/world-europe-24539417; "Ransomware Cripples IT Systems of Inland Port in Washington State," The Maritime Executive, November 19, 2020, https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state; Andrew Tsonchev, "Troubled Waters: Cyber-Attacks on San Diego and Barcelona's Ports," Darktrace (blog), October 4, 2018, https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports/; "Chinese Shipping Firm Infected by Ransomware," BBC News, July 26, 2018, https://www.bbc.com/news/technology-44965163; Emil Muccin, "Cyber Security at Sea," The Maritime Executive, April 21, 2016, https://www.maritime-executive.com/blog/cyber-security-at-sea; and Catalin Cimpanu, "US Coast Guard Warns about Malware Designed to Disrupt Ships' Computer Systems," ZDNet, July 9, 2019, https://www.zdnet.com/article/us-coast-guard-warns-about-malware-designed-to-disrupt-ships-computer-systems/.

[65] "About CAPEC," MITRE (website), updated April 4, 2019, https://capec.mitre.org/about/index.html.

Historical Communication/IT System Incidents among MTS Stakeholders			
Stakeholder	**Attestation**	**System**	**CAPEC-ID**
Terminal operator	Port of Antwerp	Terminal operating system (TOS)	CAPEC 163: Spear Phishing
	Port of Kennewick Ports of San Diego/Barcelona, Long Beach (COSCO Terminal)	Admin. systems	CAPEC 125: Ransomware
	Fieldwork	Electronic data interchange	CAPEC 549: Ransomware
	Unknown	PLCs in straddles	CAPEC 176: Configuration Manipulation
	Unknown	USB	CAPEC 523: Timer-Activated Malware

Table 9: Historical Communication/IT System Incidents among MTS Stakeholders

Future Work

This research, jointly conducted by the ACI and CIRI, has sought to quantify the impact of disruptions on cross-organizational, interinfrastructure dependencies. This appendix has focused on cyber-originating disruptions to the MTS at a regional and municipal level. However, prior work sponsored by CIRI focused on a detailed port view and the impact of disruptions to services provided by port stakeholder communications/IT networks. A detailed study of the impact of a GOS outage on various stakeholders as well as the impact that various stakeholders have on overall port operation may be found in CIRI's 2019 Simulation Winter Conference paper.[66] Such cross-organizational dependencies and how they affect overall port operation may be of particular interest to NATO and United States Indo-Pacific Command given programs such as the Belt and Road Initiative. Ongoing work in the communications/IT sector is looking to emulate and quantify the impact of targeted ransomware attacks on automated shipping ports. This work is actively being developed in collaboration with Ports of Auckland, New Zealand, and Mandiant/FireEye industrial control system team members.

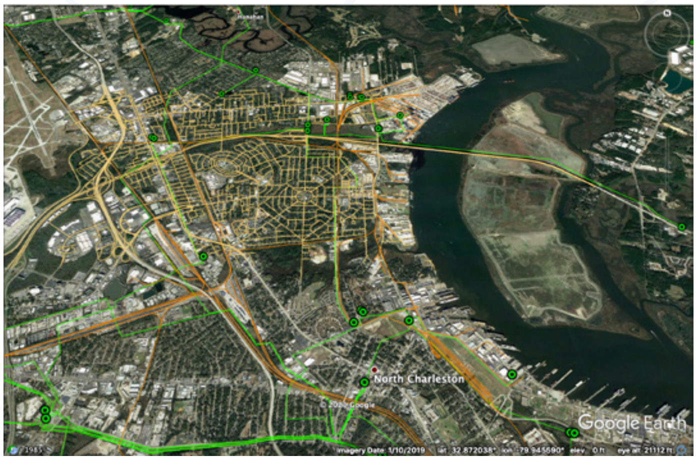


Figure 37: Geographic Proximity of Electrical Power Lines, Substations, and Power Plants at a Regional and Municipal Level

Other scenarios could be considered that integrate additional critical infrastructure systems. For example, the work of the Defense Advanced Research Projects Agency Rapid Attack Detection, Isolation and Characterization Systems, the testbed for which is hosted at

[66] Weaver, Van Moer, and Salo, "Stakeholder-Centric Analyses."

UIUC, could be integrated to analyze the impact of cyberattacks on the electrical power grid in the context of the MTS. Figure 37 illustrates the geographic proximity of electrical power lines, substations (dark-green points), and power plants (lime-green points) at a regional and municipal level. Note that the North Charleston Terminal has its own biomass power plant, according to the available DHS HIFLD data. Such research would also build on previous work by Weaver to model cyber-physical dependencies within the bulk electric power system, with a focus on protection schemes.[67]

Conclusions

The MTS accounts for more than $4.6 trillion of annual economic activity—nearly a quarter of the U.S. gross domestic product.[68] Preparing for a major disruption is key to building resilience for such critical infrastructure.

The PDT provides stakeholders with the ability to accurately model commodity flows through a shipping port, introduce a wide range of cyber and/or physical disruptions, and calculate various economic impacts of such disruptions. The PDT enables stakeholders to quantify the impact of cross-infrastructure, interorganizational disruptions in an evolving natural and man-made environment. To conduct the research presented in this appendix, CIRI extended the PDT to include fort to port. The supporting framework used to provide analyses such as this one is readily applicable to other municipalities, such as Savannah, GA, and other commercial strategic seaports.

[67] Gabriel A. Weaver et al., “Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case,” in 2016 IEEE International Conference on *Smart Grid Communications (SmartGridComm)* (New York City: Institute of Electrical and Electronics Engineers, 2016).

[68] Martin Associates, *2018 National Economic Impact of the U.S. Coastal Port System* (Alexandria, VA: American Association of Port Authorities, March 2019).

APPENDIX J – REQUIRED DELIVERY DATE (RDD) SIMULATION

In force projection operations, the RDD is a critical factor for commanders. The RDD is the date when commanders need their unit's equipment in the theater of operation to effectively execute their missions. Should equipment not arrive by the RDD, commanders are forced to consider alternative options that may not prove advantageous for timely and effective mission accomplishment. During JV 3.0, cyber incidents caused both physical and electronic disruptions to commercial critical infrastructure required to ensure equipment meets the RDD suspense. The RDD simulation seeks to inform commanders about potential impacts to RDD when conducting force projection operations in a contested environment.

For the JV 3.0 scenario, a brigade-sized task force with approximately 2,300 pieces of equipment was tasked to deploy overseas in a Sealift Emergency Deployment Readiness Exercise. The hypothetical orders to initiate the exercise came on April 29, 2020 (turn 0), with an RDD of June 1, 2020. This simulation analyzes two potential alternatives after the events of turn 5 in JV 3.0. During this turn, the ports in both cities were forced to close due to cyber and physical issues. The various incidents that led to this closure included traffic congestion, protests, cyber incidents creating delays for both rail and line haul equipment, and the listing of a ship in port that resulted in the spillage of containers. Given these events, this simulation explores the number of days associated with two primary alternatives: waiting for the original port to remediate physical and cyber issues or relocating to a new port. The goal of the simulation is to generate a distribution that describes the number of days and to develop probabilities associated with the original RDD of June 1, 2020.

The simulation will take a standard Monte Carlo approach to estimate the total number of days it takes to execute key processes. The processes involved governing the options required to handle equipment stranded at the original port, equipment that was moving to the original port, and equipment that was yet to depart. Each of the key processes are represented with a triangle distribution whose parameters (minimum, maximum, and mean) were informed by data collected during the JV 3.0 events and from discussions with participants postevent. Table 10 provides brief descriptions of the various processes and their parameters used in the simulation.

Process	Definition	Units	MIN	MAX	AVG
Fix Traffic	Time to relieve traffic congestion in area	Days	0.25	2	0.5
Fix Protests	Time for protests to dissolve	Days	0.083	1	0.333
Rail Mvmt	Speed at which rail moves to/from port	MPH	10	80	55
LH Mvmt	Speed at which trucks move to/from port	MPH	52	60	55
Cnvy Mvmt	Speed at which military convoys move	MPH	35	55	40
Recont New SPOE	Time to recontract/find a new port	Days	3	7	5
Recont New Rail	Time to recontract rail for a new port	Days	1	7	3
Recont New LH	Time to recontract trucks for a new port	Days	3	10	7
Replan New Cnvy	Time to plan new convoy movement	Days	1	7	3
Remediate Org.	Time to clean malware infections	Days	2	6	3
Reconfig Rail	Time to prepare equipment for movement	Days	2	10	3
Reconfig LH	Time to prepare equipment for movement	Days	0.75	5	1
Reconfig Cnvy	Time to prepare equipment for movement	Days	1	10	3
Port Ops	Time to load equipment onto vessel	Days	1	3	2
Fix Port IT	Time to clean malware from IT systems	Days	1	7	2
Fix Channel	Time to clear channel of debris	Days	6	21	7
Sail to SPOD	Time for vessel to sail to SPOD	Days	5	14	7

Table 10: Key Processes and Their Parameters

The ACI looked at two options for each alternative. The process diagram for each alternative is shown in figure 38. For the alternative of remaining at the original port, there is a simulation that governs container spillage into the channel and an option that focuses only on remediating the various incidents, without including the spillage. In the case of relocating ports, the ACI presents the results of moving to ports both 200 and 1,000 miles from the point of departure. The following sections discuss the assumptions and results associated with each alternative.

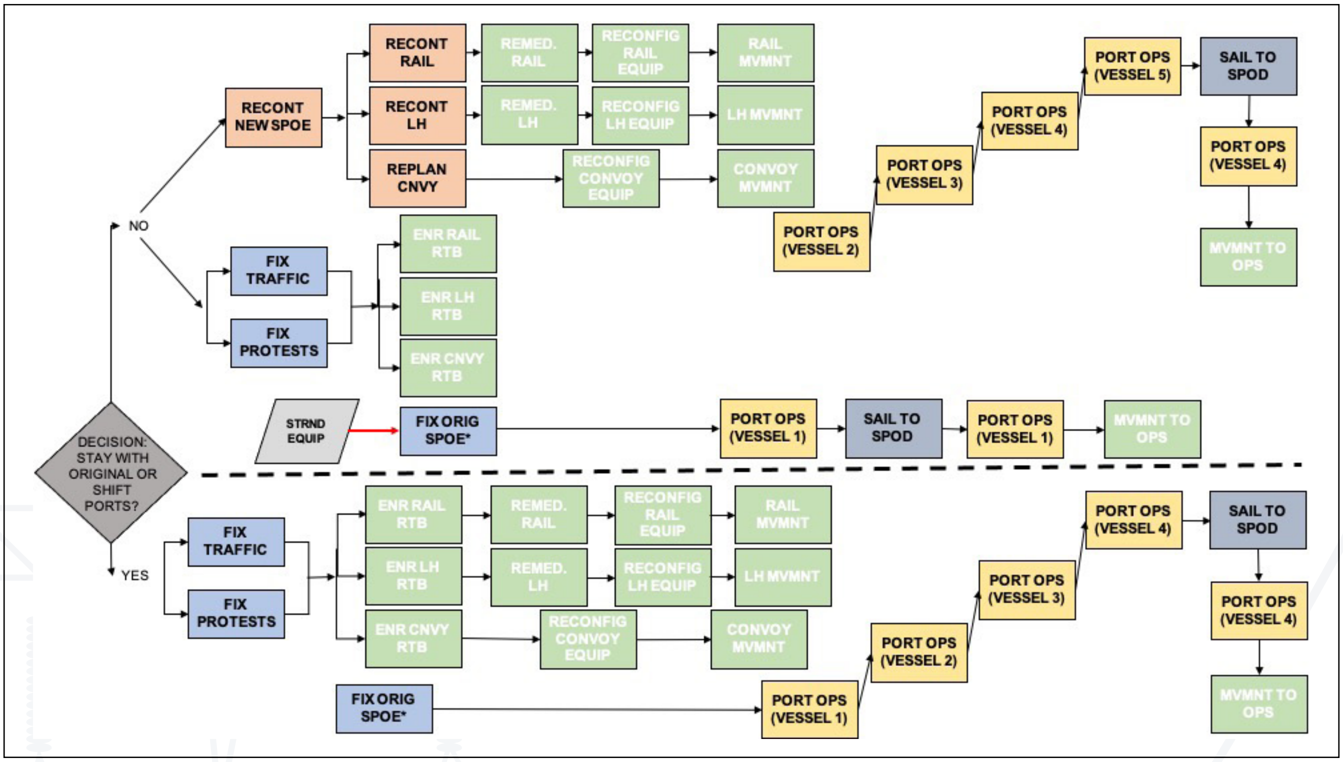


Figure 38: Process Diagrams for the Two Alternatives

J.1. Results: Remain at Original Port

For our first result, we look at staying with the original port, given the requirement to clear the channel. In this alternative, equipment that is at the port remains, and equipment moving to the port will have to return after traffic and protest issues have been resolved. We assume that movement to the port will not begin until the port is reopened, which includes establishing physical security, remediating malware, and clearing the channel. The remediation, reconfiguration, and movement for both rail and line haul occur in series, but are compared in parallel. We ran 10,000 simulations using 50 miles as the distance from point of origin to the port. In figure 39, a histogram of the results is shown on the left, and the minimum, maximum, and mean for each process is shown on the right.

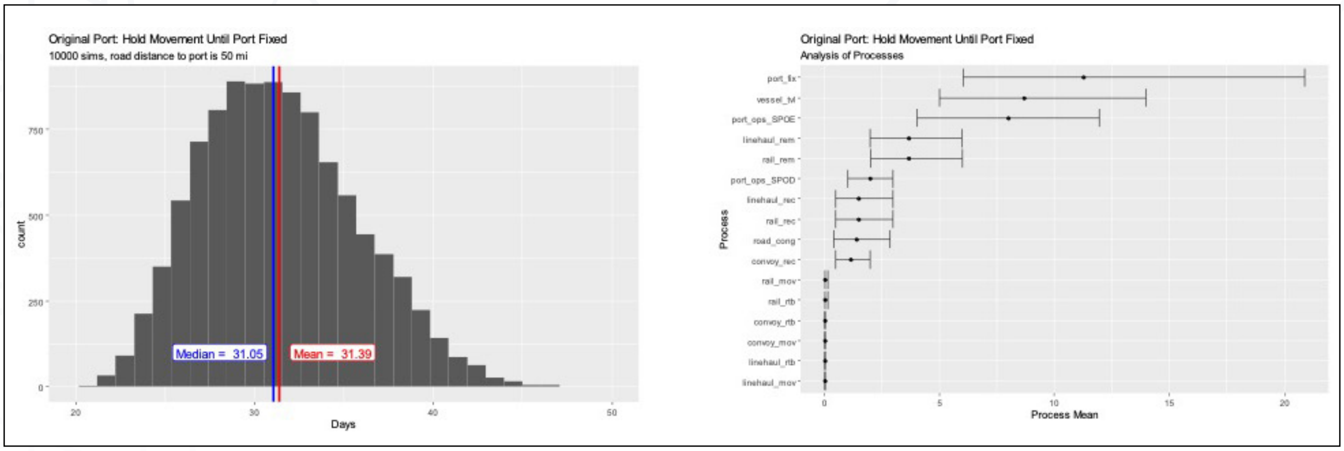


Figure 39: Original Port: Hold Movement until Port Has Been Fixed

Using the histogram, we can calculate the probability that the equipment will make RDD by summing up the number of simulations that occurred in less than or equal to 28 days (the number of days until June 1, 2020). In this case, there is a 23.4-percent chance that the equipment will make it by June 1, indicating that the scenario successfully disrupted force projection operations. Figure 39 illustrates that fixing the port (malware remediation and clearing the channel) is the most time-consuming process associated with this alternative.

Table 11 includes probabilities for additional days, indicating that it requires at least 40 days (arrival date of June 13, 2020) for a 95-percent probability.

Days	25	28	30	35	40	45	50
Prob. Make RDD	0.0519	0.2344	0.4026	0.7951	0.9692	0.9993	1.000

Table 11: Fixing the Port: Travel Times and Associated Probabilities

Our second option for this alternative is to look at a situation in which there are no issues with the channel. In this case, we have removed a significant physical effect of the cyber intrusion to determine how much impact remediating the other intrusions (traffic lights, rail failure, and truck crash) will have on RDD. Using the same assumptions as before, we ran 10,000 simulations using 50 miles as the distance from point of origin to the port. Figure 40 shows a histogram of the results on the left and the minimum, maximum, and mean for each process on the right.

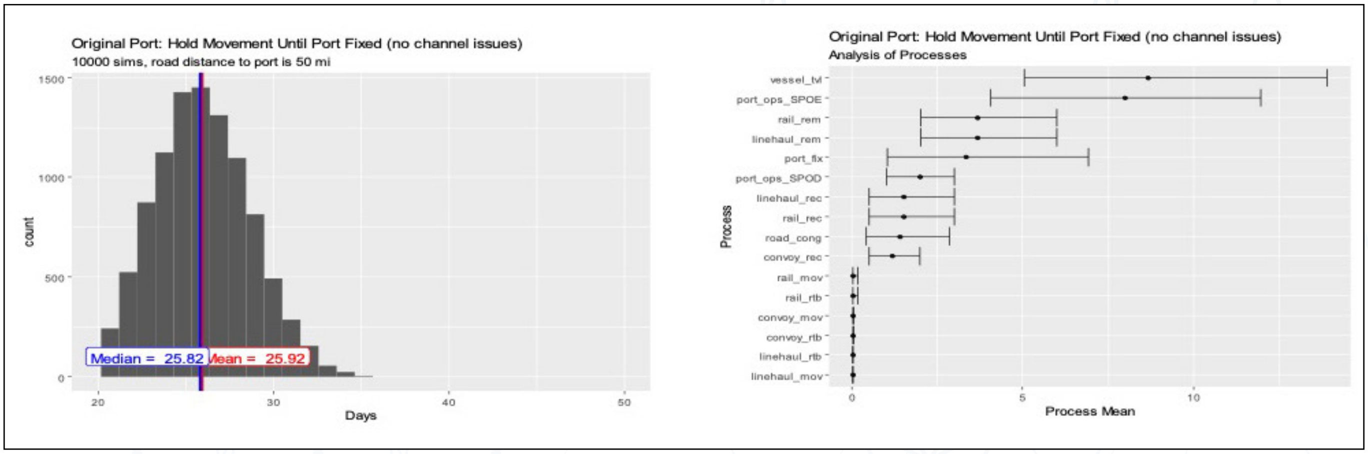


Figure 40: Original Port: Hold Movement until Port Has Been Fixed (No Channel Issues)

In this situation, we see there is a 77.25-percent chance that the equipment will make it by June 1, indicating that the scenario (minus channel issues) created some disruption to force projection operations. Table 12 provides probabilities for additional days, showing that the probability goes above 90 percent for 30 days.

Days	25	28	30	35	40	45	50
Prob. Make RDD	0.3813	0.7725	0.9263	0.9996	1.000	1.000	1.000

Table 12: Fixing the Port (No Channel Issues): Travel Times and Associated Probabilities

In terms of the processes, we see that vessel travel and the port operations at the original port take the most time. The remediation of commercial assets (rail, line-haul, and port IT) follow as most time-consuming and with the most variance.

J.2. Results: Shift to a New Port

This result looks at the alternative in which the commander chooses to shift ports. The first case considers the new port to be 200 miles away. For this alternative, we assume that the identification of a new port occurs first, followed by adjustment of the contracts for both rail and line haul (as well as convoy planning). Based on the parameters for the distributions, traffic congestion and return-to-base movement are dominated by replanning the new port and therefore are not considered. The remediation, replanning, reconfiguring, and movement for rail, line haul, and convoy occur in series. Finally, we assume that the equipment stranded at the original port will make it to the seaport of debarkation at the same time as or before the other equipment. Again, we ran 10,000 simulations and produced a graphic (figure 41) showing a histogram of the results on the left and analyses of the processes on the right.

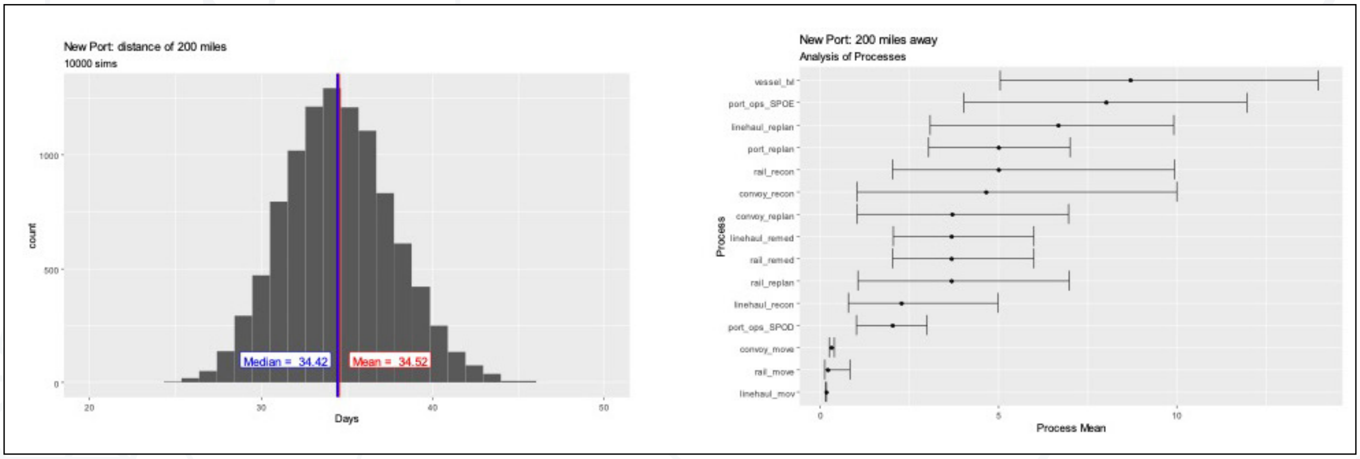


Figure 41: New Port: 200 Miles Away

For this alternative, there is a 1.28-percent chance that the equipment will make it by RDD, with over 95-percent probability of it occurring after 40 days (June 13). It follows that shifting to a port further away will reduce the probability; for a port 1,000 miles away (e.g., shifting from Charleston to Beaumont, Texas), there is a less-than-1-percent chance that the equipment will make RDD. Table 13 shows a breakdown of the probabilities by days for the port 200 miles away as well as the port 1,000 miles away.

Days	25	28	30	35	40	45	50
Prob. Make RDD (200)	0.0003	0.0128	0.0710	0.5736	0.9546	0.9993	1.000
Prob. Make RDD (1,000)	0.0000	0.0018	0.0164	0.3249	0.8516	0.9940	1.000

Table 13: New Port: 200 Miles and 1,000 Miles Away – Travel Times and Associated Probabilities

Looking at the process analysis, replanning and reconfiguration dominate the time line, with reconfiguration taking a longer time than in option 1. Though the time for the movement processes increases and adds to the delay, the replanning and reconfiguration still take the longest after vessel movement and port operations.

J.3. Conclusions

Based on this simulation of the events occurring after turn 5, we find that cyber incidents do have an impact on force projection in a contested environment. Although the alternative that relied on the original port was preferable to the one that required changing ports, it still did not guarantee the equipment would make RDD. Yet, commanders should consider the significant time investment required for relocating to a different port and seek ways to improve the probabilities associated with the original port alternative. The conclusions from this simulation are as follows.

1. Proactive cybersecurity: The physical event resulting from the cyber incident created the most significant delay in the original port alternative. Stakeholders must remain proactive and identify potential threats early, before they fester.
2. United States Coast Guard (USCG): In the event of a deployment, SDDC and deploying units must ensure they notify the USCG unit responsible for the targeted port. The USCG cyber assets can assist in security, detection, and prevention.
3. Though shifting ports seems to be the least favorable option, if a spillage includes potentially hazardous materials, then the time required to clear the channel will increase. This information should be considered a commander's critical information requirement.
4. Shifting ports may result in follow-on attacks, creating a cascading effect (recreating the situation at subsequent ports and adding to the delay).

J.4. Source Code

The source code used in this simulation is available by request to ACI.JackVoltaic@westpoint.edu.

APPENDIX K – DSCA/DSCIR

Directive-Type Memorandum 17-007 details the Department of Defense's (DoD's) approach to using defense coordinating elements (DCEs) or officers (DCOs) for cyber capabilities on a regional basis. Defense Support to Cyber Incident Response (DSCIR) is provided within the framework of Defense Support to Civil Authorities (DSCA) and may include direct, on-location support; remote support; or a combination of both. To protect, prevent, and mitigate great property damage and human suffering, DoD cyber teams are permitted to: (1) gain familiarity with critical infrastructure networks and systems; and (2) assist critical infrastructure owners or assets that are essential for the functioning of a society and economy.[69]

Role of the DCE/DCO: The DCE/DCO will be the DoD representative and liaison to the federal lead agency in the disaster area and provide situational awareness to DoD agencies. The DCE/DCO also serves as liaison to senior leaders and state, local, and other federal agencies; validates the Resource Request Form; and accepts the mission assignment from the federal coordinating officer. DCEs/DCOs assist with receiving, staging, onward movement, and integration of units/personnel; recommend military resources to meet request requirements; forward mission assignments to United States Northern Command (USNORTHCOM); provide a link to the base support installation; coordinate administrative and logistical support to deployed military forces; control small DoD units and resources in the disaster area; and maintain accounting records for reimbursement (with U.S. Army Deputy Chief of Staff G-8 augmentation).

Charleston and Savannah would be covered by a DCE/DCO under Federal Emergency Management Agency Region IV, which consists of all eight of the southeastern states (Alabama, Florida, GA, Kentucky, Mississippi, North Carolina, SC, and Tennessee). The DCE/DCO's mission is broad and encompasses support to any federal lead agency that is conducting homeland defense operations or DSCA support within the USNORTHCOM area of responsibility. Mainly, this DCE/DCO group is solely responsible for validating and processing requests for DoD assistance in coordination with and in support of the primary federal and state agencies. DHS is embedded in 10 of the critical infrastructure sectors.

Requesting DSCIR: When a request for DSCIR is received and approved, DCEs/DCOs will carry out DSCIR as directed in DoDD 3025.18 and DoDI 3025.21, Defense Support of Civilian Law Enforcement Agencies, and will be evaluated using C.A.R.R.L.L. (see section 4.2.4 of this report).[70] Legal documents, such as memoranda of understanding (MOUs), memoranda of agreement, nondisclosure agreements, or other appropriate legal documents requested by the DoD, must be signed and written acknowledgment and permission giving DoD access to provide support must be given before DSCIR is provided.[71]

[69] Work, *Interim Policy and Guidance.*

[70] Lynn, *Defense Support to Civil Authorities (DSCA);* and Department of Defense (DoD), *Defense Support of Civilian Law Enforcement Agencies,* DoD Instruction 3025.21 (Washington, DC: DoD, updated February 8, 2019).

[71] Work, *Interim Policy and Guidance.*

Federal military commanders and DoD component heads and civilians may accept federal requests for DSCIR under immediate response authority in support of a cyber incident response.[72] Industrial control systems and their supervisory control and data acquisition (SCADA) capabilities are often quite advanced, but are likely to run out of personnel and resources quickly. United States Strategic Command, USNORTHCOM, and United States Pacific Command commanders have the following responsibilities:

- Planning and executing DSCIR operations in coordination with the chairman of the Joint Chiefs of Staff (CJCS) and the combatant commanders;
- Incorporating DSCIR into joint training and exercise programs in coordination with the CJCS and in consultation with the appropriate federal departments and agencies and the National Guard;
- If they have been designated as the supported commander, coordinating with supporting DoD components to distribute all reimbursement for assistance received;
- If they have been designated as the supported commander, coordinating with the CJCS, the assistant secretary of defense for homeland defense and global security, and any supporting commands on military preparations and operations; and
- Informing the secretary of defense, through the CJCS and by the most expeditious means possible, of any actions taken to provide immediate response to save lives, prevent human suffering, or mitigate great property damage.[73]

DoD recommendations: The DoD cyber team recommends the following to prepare and protect assets in the event of a major cyber incident.

When requesting DSCIR support, a civil authority must consider the following questions:

- Who at state level is the decision maker for requesting federal cyber support?
- Where can a DSCIR request be injected into the DoD enterprise?
- Should USNORTHCOM integrate DCOs/DCEs into the validation process or retain them at USNORTHCOM?
- How do supported combatant commands from USNORTHCOM ensure situational awareness and unity of effort when Title 10 forces are being employed?
- Would this scenario amount to a “significant cyber incident” (see definition below), therefore requiring the activation of the executive Unified Coordination Group and centralized control?
    - » “Significant cyber incident. A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.”[74]

[72] Work, Interim Policy and Guidance.

[73] Work, Interim Policy and Guidance.

[74] Barack Obama, *United States Cyber Incident Coordination*, Presidential Policy Directive 41 (Washington, DC: The White House, July 26, 2016).

In addition, one must consider the following preparations to avoid or safely resolve a major cyber incident:

- Ensure teams possess a high level of expertise in the cybersecurity of traditional IT as well as operational technology (OT) systems;
- Assess force structure and team composition;
- Standardize critical infrastructure training and equipping; and
- Enhance expertise through exercises that integrate government, academia, and public and private sector cybersecurity professionals.

ARMY CYBER INSTITUTE AT WEST POINT

FTI CONSULTING™

cyber.army.mil

@ArmyCyberInst @ArmyCyberInstitute armycyberinstitute armycyberinstitute