JACK VOLTAIC

Critical Infrastructure and Public-Private Partnerships

PREPARE ■ PREVENT ■ RESPOND

Research Report

Patrick Bell | Army Cyber Institute

Daniel (Dan) Bennett | Army Cyber Institute

Robert (Bob) Butler | AECOM

Judy Esquibel | Army Cyber Institute

Courtney Gordon-Tennant | Army Cyber Institute

Andrew (Andy) Hall | Army Cyber Institute

Rhett Hernandez | Army Cyber Institute

Mary Kavaney | Global Cyber Alliance

Terence Kelley | Army Cyber Institute

Erik Korn | Army Cyber Institute

Frank Kramer | Scowcroft Center for Strategy and Security

Joshua Lawton-Belous | Global Cyber Alliance

Fernando Maymi | IronNet Cybersecurity

Erica Mitchell | Army Cyber Institute

Jonathon Monken | PJM Interconnection

Michael Nowatkowski | Augusta University

Brian Nussbaum | State University of New York at Albany

Joseph (Joe) Pfeifer | Harvard Kennedy School

ARMY CYBER INSTITUTE AT WEST POINT

EDITORS:

Patrick Bell | Army Cyber Institute

Natasha Cohen | New America

Judy Esquibel | Army Cyber Institute

Courtney Gordon-Tennant | Army Cyber Institute

Erica Mitchell | Army Cyber Institute

Michael Nowatkowski | Augusta University

Brian Nussbaum | State University of New York at Albany

Glenn Robertson | Army Cyber Institute

David (Michael) Thomas | Naval Postgraduate School

SPECIAL THANKS TO:

New York City, the City of Houston, public-private sector partners and contributing members (listed in alphabetical order): Hong Ablack, Art Acevedo, Mike Allgeier, Melanie (Mel) Bartis, Patrick Bell, Joshua Lawton-Belous, Alison Beltcher, Daniel (Dan) Bennett, Lisa Beum, Theresa Blackwell, Pete Bosse, Justin Breeding, Geoffrey (Geoff) Brown, Jeffrey S. Buchanan, Arielle Budoff, George Buenik, Robert (Bob) Butler, Eric Coffey, Natasha Cohen, Michael Davis, Mary Dickerson, Judy Esquibel, John Esquivel, Larry Ewert, Greg Frisinger, Irina Garrido de Stanton, John Giordano, Julio Gonzalez, Courtney Gordon-Tennant, Scott Hagerty, Andrew (Andy) Hall, Jack Hanagriff, Tom Harrington, Chris Hartley, Bob Harvey, Laura Henriquez, Jordan Henry, Rhett Hernandez, Arthur Hudman, Chris Humphreys, William Hutchison, Henry Jackson, Pablo Jacobs, Bob Janusaitis, Trameka Jewett, Rich (Stella) Johanning, Mary Kavaney, Andjelka (Angie) Kelic, Terence Kelley, Todd Kimbriel, Erik Korn, Frank Kramer, Laura Lee, Yosef Lehman, Bridget Lindem, Victor (Vic) Macias, Fernando Maymi, Austin Minter, Chris Mitchell, Erica Mitchell, Jonathon Monken, Mel Nevarez, Michael Nowatkowski, Daniel Nunez, Brian Nussbaum, Tom O'Brien, Chris Perkins, Joseph (Joe) Pfeifer, Brian Rexroad, Glenn Robertson, Gustavo (Gus) Rodriguez, Bertrand Sausseiii, Jessica Schein, Michael Stone, Sumit Singh, Sylvester Turner, Chet Ung, Umesh Verma, Michael (Mike) Vicente, Tony Vitello, Guy Walsh, Greg White, Paul Winter.

CONTENTS

THE ATTACK SCENARIO

A city is experiencing an increasing number of seemingly random incidents. A major financial institution suffers system failures, sending shockwaves through the markets. Workers struggle to keep the public transportation system operating as critical control systems fail. Social media reports of terrorist attacks incite panic. The city's first response capability begins to strain. Regional medical facilities are at capacity. The media struggles to inform an increasingly concerned public. Elected leaders and emergency response leadership gather in the city's emergency operations center to analyze the situation and respond.

A sinister reality emerges when a foreign terrorist group claims that the city is under siege from cyberspace.

1. INTRODUCTION

This report summarizes the U.S. Army Cyber Institute's (ACI's) work to date on Jack Voltaic (JV), a research project that focuses on critical infrastructure and public-private partnerships (PPPs). JV research, which includes contributions from academia, industry, and government, explores how to synchronize Department of Defense (DoD)/U.S. Government and private sector capabilities in a cyberspace attack response. JV is a research framework that enables the Army to recognize the impacts of cyberspace operations from a municipal and critical infrastructure perspective.

Now more than ever before, the need for infrastructure resilience is extremely important. Digital connectivity makes our infrastructure more efficient and, simultaneously, more vulnerable. However, critical infrastructure need not be connected to the Internet to be vulnerable. Cyberspace attacks rarely affect a single target. Instead, unanticipated effects often ripple across interconnected infrastructure sectors. Varying defensive capabilities and authorities complicate the response. If exploited by a determined adversary, these unidentified gaps leave the Nation vulnerable. By simulating attacks on the infrastructure critical to a city's functioning and by examining the reactions of infrastructure owners and operators, emergency services, and security officials, the JV experiment/exercise environments served to create new data and datasets that the Army can use to assess the consequences of cyber incidents.

JV began as a way to explore implementing "cyber mutual assistance," a concept stemming from longstanding energy sector practices.[1] Within the energy sector, mutual assistance provides a common framework for electrical utilities to use in mobilizing assets and capabilities from across the Nation to respond to a major incident, such as a natural disaster that causes widespread power outages.

The ACI, which has conducted JV research for the past 3 years, performed cyber exercises JV 1.0 in New York City (NYC) 29-31 August 2016 and JV 2.0 in Houston 24-26 July 2018.

Through the JV project, the ACI, alongside its assembled partners, aims to identify gaps, identify interdependencies among critical infrastructure sectors, and provide recommendations for improvement. JV also provides an innovative, bottom-up approach to critical infrastructure resilience. The ACI, an organization within the DoD and Federal Government, serves primarily as an advisor and facilitator in these exercises/experiments. Because the ACI is recognized for its roles in academia and in providing strategic-level thinking, it is an ideal organization for instilling trust and facilitating the involvement of participants from multiple sectors.

This report highlights the value of the ACI's JV research to local municipalities, their infrastructure partners, the Army, the DoD, and the Nation. It is critical that the ACI share in an open and transparent way the lessons learned from JV, both to raise the quality of discussions and debate around these issues and to improve the resilience of the critical infrastructure that the DoD relies on to defend the Nation and conduct military operations.

[1] Jonathon Monken, Fernando Maymi, Dan Bennett, Dan Huynh, Blake Rhoades, Matt Hutchison, Judy Esquibel, Bill Lawrence, and Katie Stewart, *Cyber Mutual Assistance Workshop Report*, Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute, 2018, available from *https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_513596.pdf.*

The ACI's JV research enables the Army to explore cyberspace operations from the perspective of a municipality and in conjunction with the web of infrastructure sectors that make that city function. JV 1.0 was the first step in building a framework for preparing for, preventing, and responding to multi-sector cyberspace attacks on major cities. JV 2.0 explored the employment of the total Army force to defend the Nation in the face of an advanced physical and cyberspace attack on a major U.S. port city and the cyber resilience and readiness of Army-operated Defense Critical Infrastructure to support military force projection and sustainment from the port city. Because the purpose of the JV research framework is to iterate multiple exercises – some with similar characteristics and some with different ones – in order to build pictures of the various impacts and interdependencies that knit cities together with their infrastructure partners, JV 2.0 naturally built on the experiences and insights gained from JV 1.0.

As a direct result of JV 2.0 research, the 2019 National Defense Authorization Act (NDAA), Section 1649, directed the DoD (Assistant Secretary of Defense for Homeland Defense and Global Security) to implement a pilot program that would simulate cyberspace attacks on critical infrastructure in order to identify and develop means for improving DoD responses to requests for defense support for civil authorities in response to such attacks.

The JV project's strategic impact shows that the highest levels of government recognize the Nation's need to establish preparedness for inevitable national disasters and cyberspace attacks through these exercises. The aftermath of tragic events highlights the necessity of sectors such as first responders and emergency management to share their information for public safety. JV provides a forum where stakeholders can meet in a low-threat environment, instead of waiting for a catastrophic event such as 9/11 to forge these critical relationships and organize their responses.

1.1. The U.S. Army Cyber Institute (ACI) at West Point

The ACI conducts high-quality research on the Army's most critical cyber-related challenges to bridge gaps by performing outreach and to promote information exchange across Army, military, academic, industry, and government cyber communities. The ACI supports the Army and the Army's cyber community in providing future recommendations and their current implications. The ACI analyzes today's public and private trends in technology and talent management development to be prepared for tomorrow's challenges. Our efforts support the force proponent with insights and recommendations. Our research will enable programs to plan for future threats and possibilities, and the partnerships we develop through our work will enable collaborative efforts going forward.

The mission of the ACI is to be a national resource for interdisciplinary research, advice, and education in the cyber domain, engaging DoD, Army, government, academic, and industrial cyber communities in impactful partnerships to build intellectual capital and expand the knowledge base for the purpose of enabling effective Army cyber defense and operations.

Defense of the Nation depends on the ability to rapidly process and share information. Modern communications process most information through the Internet, which is mostly privately owned and operated and used by for-profit organizations, not-for-profit organizations, academic institutions, and government agencies for research, commerce, the provision of services to citizens, and the sharing of information. The Army must partner with these outside entities to develop solutions for operating in this space that support our national defense.

1.2. ACI Partnerships

The ACI accomplishes its mission by working with partners on problems of mutual interest. Preparing for and preventing future cyber conflict requires public-private work by experts on critical topics which can facilitate future successes. Academic and industrial partnerships allow the ACI to work with experts from across multiple communities in support of research critical to the cyber community.

Figure 1: The Cyber Defense Review

The greatest challenge facing the ACI is identifying future threats to the cyber community before they can negatively impact our military forces or partners. To do so, we must leverage the collective research and development (R&D) of our industrial base as well as collaborate with the owners of our country's critical infrastructure and key resources (CIKR). The ACI partners across academia, industry, and government to create teams of experts who work together on the toughest problems facing these communities. Like those working at the entrepreneurial edge, much of our work may only be appreciated in hindsight.

The ACI aims to create knowledge, expand understanding of the cyber domain, and develop partnerships. Leveraging our like-minded allies across the domain requires a community devoted to the study of cyber conflict. The ACI has supported the creation of this community by developing The Cyber Defense Review, a journal that shares peer-reviewed research and the professional commentary of insightful military, government, and industrial leaders.[2] Additionally, in cooperation with the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Center of Excellence, the ACI helped bring a premier cyber conference, CyCON U.S., to the United States.[3]

Specific to the JV project, the ACI has developed critical infrastructure industry partnerships, which are described in the following sections.

1.2.1. Importance of JV

The JV research project demonstrates the value of research on developing and leveraging strategic partnerships. JV, one of the ACI's first codified partnership efforts with industry, involved a multidisciplinary problem set consisting of legal, policy, and physical incident response challenges combined with a cyber live-fire training exercise on a network. The project, which served as a proof of concept exercise in defending the Nation, entailed understanding the role of the military in addressing a cyberspace attack as well as identifying the gaps and redundancies within response measures. This is important because JV can be used to formulate long-term plans for assessing DoD installations and to ensure that the United States can project power when its critical infrastructure is under duress.

In addition to benefiting the DoD, the JV research project provides important benefits to civilian industries – particularly, critical infrastructure owners and operators. An inadequate response to a cyberspace attack undermines public trust in industry and could damage companies' reputations, hurt short-term profits, erode their market share, and increase the demand for government regulation of their industries.

Finally, because the JV research project demonstrates dependencies and vulnerabilities, it enables cities and municipalities to understand their own capabilities as well as those of their infrastructure partners. Participants from various organizations were able to meet and exchange contact information in a calm,

[2] Army Cyber Institute, *The Cyber Defense Review*, available from *https://cyberdefensereview.army.mil/The-Journal/Publications/*.
[3] Army Cyber Institute, "CyCON U.S.," available from *https://cyber.army.mil/Events/CyCON-US/*.

low-threat environment and prospectively identify whom to call in a time of crisis. Beyond merely developing critical personal and organizational relationships, the participants became better able to understand the worldviews, expectations, interests, capabilities, and limitations of the organizations they might have to work with in a "Cyber Worst Day" scenario. The JV exercise also helps cities comply with local, state, and Federal Government regulations for conducting multiple types of emergency exercises at a single time. The exercise design utilized in JV could serve as a foundation for developing a comprehensive framework for responding to a future cyberspace attack.

1.2.2. Innovate, Experiment, and Partner

The ACI is charged with providing innovative ideas to the Army, the DoD, and the Nation in order to address future cyber-related challenges. The ACI leverages partners to enable opportunities and evolve the capability and capacity of its cyber force.

On April 8, 2016, the ACI hosted a cyber mutual assistance workshop (CMAW) led and facilitated by the ACI, the Electric Infrastructure Security Council, and Carnegie Mellon University.[4]

The CMAW, which was the initial phase of the JV research project, provided an opportunity for experts and practitioners from the public and private sectors to examine cyber mutual assistance using a holistic approach and sharing capabilities and issues concerning the energy sector. The CMAW also spawned the idea to develop an experiment.

During a cyberspace attack, the most likely response would involve coordination through federal entities, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and intelligence fusion centers. However, the management and command and control (C2) structures and processes of these organizations are still being defined and are at varying levels of maturity and capacity.[5,6] Similarly, fusion centers vary in their commitment to cybersecurity and their interconnectedness with their communities. As such, similar incidents could play out quite differently across the country, or across industries.

Figure 2: Mr. Andrew Natoli (left) and Dr. Brian H. Nussbaum (right) participating in the JV 1.0 TTX

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 the following:

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

1.3. Partnerships Involved in JV Research: Citigroup and AECOM

The ACI engaged Citigroup (Citi) and AECOM as co-leaders in planning, developing, and executing JV 1.0 and JV 2.0, respectively. As leaders in their respective industries, these organizations enhanced the research effort by contributing additional perspectives and expertise on critical infrastructure cybersecurity.

For JV 1.0, the ACI partnered with Citi because its Global Cyber Threat Exercise Team (Citi-GCTET) offered robust cyber exercise capabilities. Citi-GCTET provided development, planning, execution, reporting, and communication capabilities for strategic, tactical, and technical cyber-threat exercises and war games. Over the course of 4 months, the ACI consulted with relevant federal, state, and local entities to ensure realism, the inclusion of key players, and sufficient granularity. This process contributed

[4] *Cyber Mutual Assistance Workshop Report*, op. cit.
[5] "National Council of ISACs," National Council of ISACs Website, n.d., available from *https://www.nationalisacs.org/*.
[6] Department of Homeland Security, "Information Sharing and Analysis Organizations (ISAOs)," available from *https://www.dhs.gov/isao*.

to the eventual creation of the NYC Cyber Command, a centralized organization leading the city's cyber defense and incident response.

Following the success of JV 1.0, the ACI team developed a working partnership with the New York State Governor's office and the New York County District Attorney. This continual partnership has extended to the State University of New York at Albany, the International Association of Fire Chiefs, and the New York National Guard. Though these efforts are just beginning, they will ultimately achieve strategic initiatives to educate other communities in cyber preparedness and response. This set of partnerships and follow-on engagements, while not one of the initial taskings of the JV framework, demonstrates how organizations that share overlapping goals, values, needs, and concerns can benefit from meeting, operating together, and learning from each other in an environment that lacks the stress and tumult of a live incident.

Figure 3: CMAW Representative Bill Lawrence (Electricity Information Sharing and Analysis Center/North American Electric Reliability Corporation)

For JV 2.0, the ACI partnered with two companies, AECOM and Circadence, to build on JV 1.0 and expand the ACI's knowledge of existing cybersecurity capabilities and protection gaps. As co-lead, AECOM, a global leader in critical infrastructure resilience, conducted exercise and scenario development and surveyed all critical infrastructure organizations participating in the event. Circadence, a cutting-edge cybersecurity software development company, provided the live, virtual, constructive environment.

Figure 4: CMAW attendees Tom O'Brien and Jonathon Monken

2. JV RESEARCH FRAMEWORK

Over the course of 3 years, the ACI conducted two experiments in the form of cyber exercises: the first, JV 1.0 in NYC 29-31 August 2016, and the second, JV 2.0 in Houston 24-26 July 2018. Both JV events were local and involved multiple critical infrastructure sectors. In general, cyber exercises consist of a tabletop exercise (TTX), a live-fire exercise (LFX), or both, and incorporate a single sector or multiple sectors. The following are identified scopes of cyber exercises:

- International (e.g., Locked Shields, Crossed Swords, and Cyber Guard)
- National (large-scale, distributed, and strategic – e.g., Cyber Guard, Cyber Storm, and Cyber Shield)
- Regional (state, multi-state, or sector-specific; distributed and often strategic – e.g., National Guard Cyber Yankee event, Quantum Dawn, and Grid-Ex)
- Local (usually conducted as a TTX or LFX within a city or an organization)

Each category of cyber exercise is necessary and serves a particular objective.

2.1. Experiment/Exercise Design Concept

The ACI, as referenced in figure 6, took a bottom-up approach in developing the JV exercise by building a team of experts in the field of critical infrastructure before a scenario occurs, rather than the other way around. Instead of being directed by higher levels, each of the participants helped drive the scenario by providing feedback about what areas they wanted to focus on improving during the exercise.

Figure 5: JV 1.0 LFX Red Team members, NYC (U.S. Military Academy Faculty Team Officers in Charge and Cadet Competitive Cyber Team)

Because a "Cyber Worst Day" scenario would likely impact cities, JV considered local municipality involvement in cyber exercises. Cities are interesting actors in cyberspace because they vary widely – from megacities to small cities, digital cities to those barely computerized, regionally integrated to relatively isolated – and have widely different physical geographies and industrial concentrations. As such, cities have unique sets of threats, vulnerabilities, and consequences that emerge in an analysis of cyber incident response.

One of the key differences between JV and most other national preparedness exercises was that JV focused on areas of interest that were nominated by the participants – that is, while these exercises featured national-level capabilities and resources, they were conceptually driven by the concerns of the cities and their infrastructure partners. This approach makes sense when the JV framework is viewed as a research platform through which the ACI, the Army, and the DoD harvest insights about their potential roles, dependencies, partners, and requests that might be made of them while allowing cities to take part in an exercise that both meets their goals and helps them discover needs.

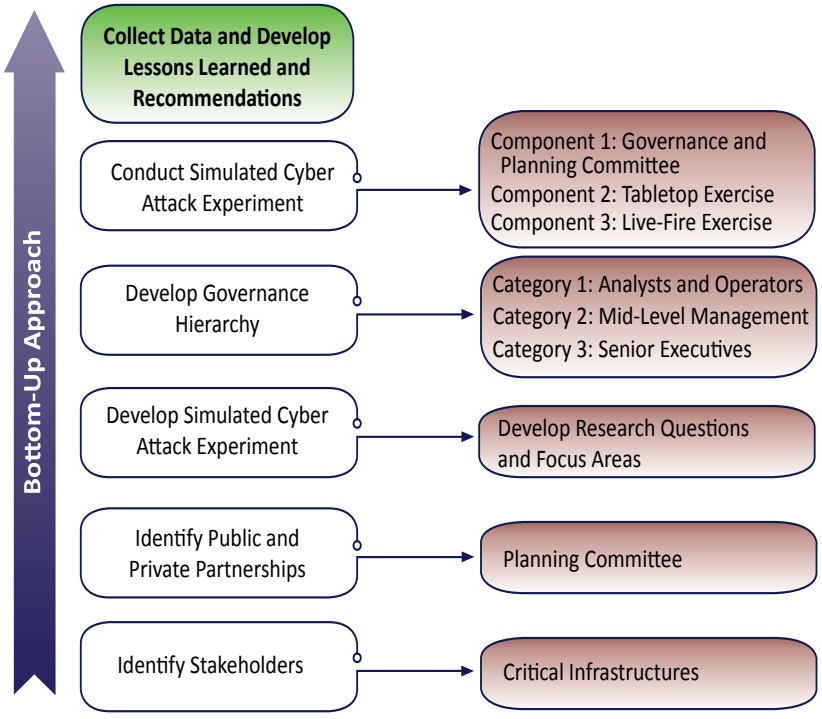

Figure 6: The ACI's bottom-up approach in developing JV

2.2. Components: Governance and Planning Committee, Tabletop Exercise, and Live-Fire Exercise

Three essential components comprised JV: the Governance and Planning Committee, the TTX, and the LFX. The Governance and Planning Committee, which was the most critical component, brought together representatives from sector-specific, critical infrastructure organizations. The LFX and TTX were cyber simulations that depended upon available resources (e.g., employees) and capabilities (e.g., access to information technology (IT), operational technology (OT), and virtual range environments). The LFX and TTX exposed participants to threat tactics, tools, and shared techniques and improved management's awareness of the potential risks and effects of a cyberspace attack.

Developing JV in this manner gave participants in all three of the components an opportunity to conduct collective cybersecurity training. The training enhanced cross-sector information sharing practices and helped facilitate technical-level threat information sharing.

Figure 7: JV components were inspired by existing exercise frameworks

2.2.1. Component 1: Governance and Planning Committee

The Governance and Planning Committee is comprised of representatives from sector-specific, critical infrastructure organizations. Committee members, also known as "trusted agents," are key to successful development and execution.

The planning committee held monthly planning meetings and hosted bimonthly teleconferences. Committee members leveraged the All Partners Access Network, a collection of communities developed to foster information and knowledge sharing among the DoD, multinational organizations, coalitions, and nongovernmental agencies that do not have access to traditionally-restricted DoD networks.

Figure 8: JV 2.0 attendees (October 2017) - ACI initial meetings with Texas Key Leaders, Houston

The ACI collaborated with participating sectors to develop innovative ideas and objectives for exercising a coordinated response to a catastrophic cyberspace attack. The sectors involved in developing the JV

exercises also participated in them. The intent was for each sector to contribute to the creation of the exercise. Although not every idea made it to the final version of the exercise, this collaborative approach helped the planning committee develop a scenario around a simulated, catastrophic cyberspace attack that was challenging and beneficial to all of the participating organizations.

2.2.2. Component 2: Tabletop Exercise (TTX)

The TTX was a facilitated discussion that took participants through a scenario requiring them to blend their physical disaster preparations with cyberspace attack response procedures.

By bringing mid-level managers into a facilitated discussion led by a moderator, the TTX helped leaders assess their plans, policies, and procedures.

Additionally, the TTX helped familiarize participants with the response process and enabled administrators to gauge the effectiveness of their emergency response practices.

Figure 9: JV 1.0 TTX, NYC

2.2.3. Component 3: Live-Fire Exercise (LFX)

The LFX was conducted on a simulated, virtual environment to test cyber equipment and response capabilities in real time. The LFX aimed to examine and validate coordination and C2 among various multi-agency coordination centers, such as emergency operation centers.

The scenario for the LFX necessarily correlated strongly with the one used for the TTX. The tactics, techniques, and procedures employed during the LFX were consistent with an exercise plan that included a list of equipment and unit control measures, including communication plans. During LFX planning, the risk management process addressed the potential control measure hazards, aiming to reduce or eliminate them. The LFX consisted of an on-range network, virtual range environment that simulated critical infrastructure environments to enhance the training value. The LFX demonstrated the impacts of successful attacks in an operational environment, including explaining what worked for defenders.

Figure 10: JV 1.0 LFX, NYC

The LFX targeted technical analysts and operators and used opposing offensive and defensive teams in various scenarios.

In building the LFX, a realistic training environment was key to a successful exercise. The cyber range needed to be sophisticated enough for the capabilities of the participants. In order to research the OT environment, the JV exercises used a simulated Supervisory Control and Data Acquisition (SCADA) environment, a system for remote monitoring and control that operates over communication channels using coded signals, including “OT” (network) and “ICS” (industrial control system), which refer to control networks. This setup allowed participants to overcome their natural hesitation to talk about simulation outside of their standard networks.

2.3. The Players/Participants

In general, there are three levels of participants involved in a cyber exercise. These participants are divided into three categories.

- **Category 3:** Senior executives and leaders.
- **Category 2:** Mid-level management, including first-line supervisors (e.g., TTX players).
- **Category 1:** Operational – analysts and operators (e.g., virtual range/LFX players).

Due to resource limitations and conflicting commitments from stakeholders, JV 1.0 and 2.0 focused on categories 1 and 2, whereas an ideal exercise would have brought in senior executives and leaders as players, rather than as distinguished visitors who only observed a small portion of the exercise.

Although JV was inspired by existing cyber exercise frameworks, it was not restricted to any individual framework. Cyber exercises can have a limited impact on improving readiness because they have a tendency to be either too technical or too high-level from a policy standpoint. The goal of JV was to ensure that the managers, operators, and technical personnel were physically co-located and could interact with each other to develop a common understanding of the operational environment.

Both the LFX and TTX provided opportunities to conduct collective cybersecurity training and to enhance cross-sector information sharing. In JV 2.0, both the LFX and TTX mimicked a real-world response and required mid-level managers to disseminate threat intelligence received from peer organizations to operators as well as respond to threats detected by operators. This approach ensured that the exercise included collective cybersecurity training and opportunities for cross-sector sharing (including coordinated, technical-level threat intelligence sharing) and that it facilitated the communication of effects and risk with participating managers.

2.4. The Experiment/Exercise: JV 1.0 – New York City

JV 1.0 was a relatively small exercise that demonstrated a cyberspace attack in NYC impacting multiple sectors and tested the city's ability to respond. First responders, emergency managers, and workers from the transportation, telecommunications, power, water, finance, and healthcare sectors took part in the exercise.

The exercise had components occurring at both the strategic and the operational levels. It included two parallel tracks—an on-range network, defender-versus-attacker LFX, and a facilitated TTX with sector leader participants—that focused on events occurring in the virtual range play. The primary goal of the experiment was to establish a framework for multi-sector cyberspace exercises for large municipalities, to demonstrate this framework, and to test whether it could be used to gain insights into the coordination and collaboration that occurs in response to cyber incidents. This framework is currently being further developed among government, university, and industry partners with the goal of exporting and sharing it with other municipalities. While lessons learned from individual scenarios or infrastructure sectors may not be directly transferable to new cities, the broad approach of simulating cyber incidents, testing strategic and operational response capabilities, and creating data and insights should be able to improve processes across any jurisdiction or industry.

Figure 11: JV 1.0 Planning Committee members, NYC (ACI and Citigroup)

JV 1.0 Planning Committee members were selected from the emergency responder community and included representatives from the financial services, emergency services, communications, healthcare, energy, and transportation systems critical infrastructure sectors.

Figure 12: JV 1.0 LFX Red Team members (U.S. Military Academy Cadet Cyber Competitive Team, Simspace, and other observers), NYC

The JV 1.0 TTX consisted of an informal, guided conversation led by a moderator. The JV 1.0 LFX was comprised of network defenders (the Blue Team)

who defended information systems against a group of mock attackers (the Red Team). The Blue Team leveraged sensors and analysis tools on the range to detect and respond to threat activities targeting the defended network. The Red Team's objective for the exercise was to enable cyber resiliency by improving enterprise information assurance and incident response. The team did so by demonstrating the impacts of successful attacks and allowing defenders to identify best practices in an operational environment. A third team, the White Cell, controlled and facilitated engagement between the Blue and Red teams and enforced the rules of the exercise.

The purpose of the research report was to shed light on the common problem areas across multiple infrastructure sectors and make recommendations to other U.S. municipalities in order to improve their resilience in responding to a natural disaster or deliberate attack. Some findings of the JV 1.0 exercise were considered sensitive and not releasable to the public in an academic forum.

Figure 13: JV 1.0 LFX Red Team members (opposing force) New York and Maryland National Guard, NYC

JV 1.0 simulated a hypothetical cyber event in NYC involving a strategic, methodical attack by a notional adversary occurring over 6 days. The first phase of the attack impacted the financial sector through a spear phishing attack targeting a business executive. The second phase targeted the energy sector through malicious software installed on a power company's network. The malware granted the attackers remote access to the company's power stations, which were then used as a pivot point to further exploit and compromise the city's transportation tunneling and signaling systems. This in turn led to the destructive malware targeting the city's water treatment plants. Chaos was then simulated as the public became aware of the problems and coordinated physical attacks began to unfold. Subsequent explosions and active shootings across the city led to mass casualties in the scenario.

A calamitous public response followed which was amplified by the viral spread of disturbing videos and images of the ensuing violence across social media. The mobilization of fire and police departments was severely impacted because the attacker encrypted first responders' critical systems using ransomware.

2.4.1. JV 1.0 Research Objectives

The main objective of JV 1.0 was to identify a framework in which any city can rehearse coordinated responses to cyber incidents that affect multiple sectors. The exercise provided a venue in which participants could gain exposure, train players, and evaluate responses. The goal was to observe a city's ability to collaborate in a coordinated response to a cyberspace attack. Table 1 outlines JV 1.0's research goals.

Furthermore, JV 1.0 explored a city's existing intelligence and information sharing capabilities and encouraged the innovative development of cybersecurity training exercises to match the sophistication of contemporary cyber threats and cyber environments. The exercise focused on a city's prioritization and coordination of recovery efforts in order to identify interdependencies and analyze potential gaps among sectors and outstanding cybersecurity challenges.

Through JV 1.0, the ACI sought to identify strengths, weaknesses, and best practices for improving system-wide security and incident response and to increase awareness of and insight into the cyberspace attack response challenges facing infrastructure sectors. The ACI also sought to expose city officials and industry or infrastructure partners to, and familiarize them with, each other's perspectives, processes, and response capabilities. This was important because a more realistic understanding of what partners bring to the table can translate into more realistic planning that better reflects real organizational capacities.

JV 1.0 Research Objectives	
1	Assess a city's response capabilities through a multi-sector cyber exercise at the local level, including intelligence and information sharing mechanisms, incident management structures, and decision-making authorities and coordination.
2	Determine whether a city's cyber crisis management planning is sufficiently integrated with physical crisis management planning, including public, private, and public-private coordination, during a cybersecurity crisis.
3	Develop a replicable framework for a city's response to a cyberspace attack impacting multiple sectors.

Table 1: JV 1.0 Research Objectives

2.4.2. JV 1.0 Timeline

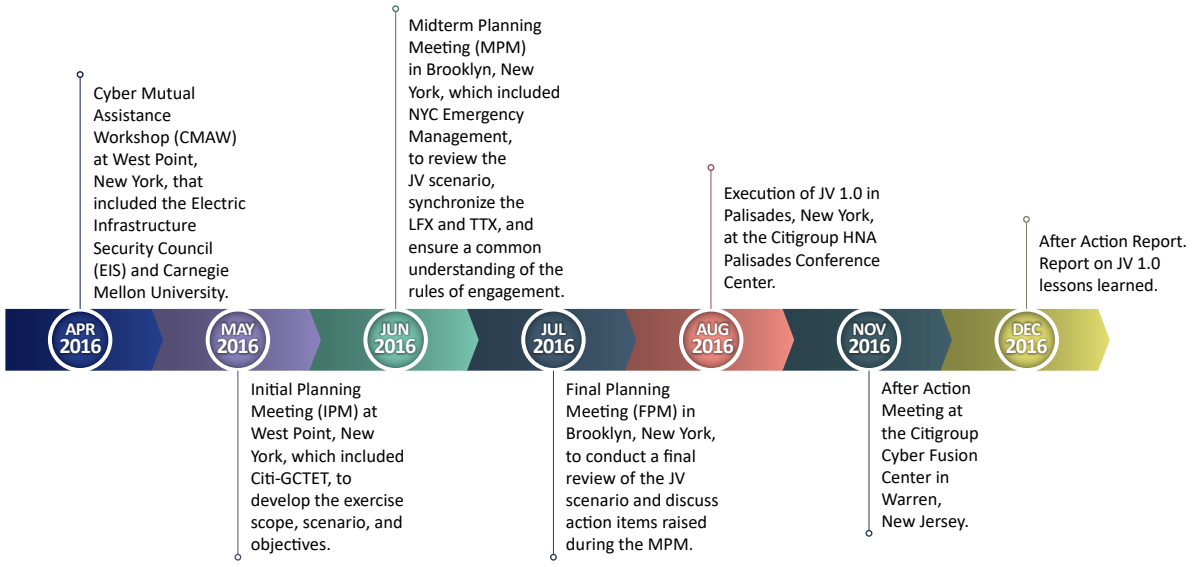

Figure 14: JV 1.0 Timeline

2.5. The Experiment/Exercise: JV 2.0 – Houston

Like its predecessor, JV 2.0 was a multi-sector, public-private, cybersecurity research project that culminated in a 3-day exercise. The exercise explored how a large city would respond to simultaneous physical and cyberspace attacks that impacted multiple critical infrastructure sectors. The project advisors included planners and operators from multiple Army commands; major infrastructure sectors; and various local, state, and federal agencies.

Figure 15: JV 2.0: Port of Houston

JV 2.0 in Houston explored the employment of the total Army force to defend the Nation in the face of physical and cyberspace attacks on a large U.S. port city, the cyber resilience of Army-operated Defense Critical Infrastructure, and its readiness to project military power and sustain operations abroad from the port city.

Figure 16: Senior leaders from public and private organizations observed the exercise and discussed efforts for improving cyber resiliency.

JV 2.0 integrated the defense industrial base sector and involved seven additional critical infrastructure sectors: emergency services, energy, healthcare and public health, transportation, communications, water and wastewater, and government facilities. JV 2.0 aimed to accomplish multiple shared objectives for the ACI, U.S. Army Cyber Command (ARCYBER), U.S. Army North, and U.S. Army Surface Deployment and Distribution Command (SDDC). In particular, it sought to improve the Army's overall awareness of cyber threats and interdependencies as well as increase Defense Critical Infrastructure resiliency. Through the exercise, the Army would ideally be better informed to develop future cyber capabilities, force structures, and procedures for responding to cyber-physical attacks. By bringing so many stakeholders together, the exercise also contributed to the achievement of Army and DoD installation mission assurance objectives.

The exercise enabled the Army to better understand private sector and government responses and procedures for identifying gaps and defending cyber key terrain.

With an increased number of infrastructure sectors and Army stakeholders represented, JV 2.0 provided a more complex response environment and offered new insights that built off of those gained from JV 1.0. The JV framework has proven to be sharable and exportable, leveraging different insights depending on where and by whom it is used.

A major addition for JV 2.0 was integrating the National Guard due to the vital role it serves in the Nation's cybersecurity. JV 2.0 directly supported the National Guard's 2018 Cyber Strategy by enabling shared situational awareness and response capabilities among mission partners, working with federal agencies to support and improve cybersecurity and resilience in the homeland, engaging state mission partners to secure and defend cyberspace, pursuing engagements with public and private-sector mission partners, and partnering with academia on mutually beneficial training and research opportunities.

JV 2.0 centered around a hypothetical scenario in which a hurricane and cyberspace attack simultaneously struck in and around Houston. Technical experts and executive leaders representing critical infrastructure, regional emergency management, and state and federal agencies collaborated on a TTX and an LFX. During the TTX, facilitators guided discussions on response actions and challenges. The LFX provided a virtual cyber environment in which technical experts tested their skills against adversarial threats.

2.5.1. JV 2.0 Research Objectives

The four main research objectives of JV 2.0 are outlined in table 2.

JV 2.0 Research Objectives	
1	Develop a framework in which to exercise a city's ability to respond to a combined physical attack (e.g., a natural disaster) and cyberspace attack affecting multiple infrastructure sectors.
2	Evaluate the cyber resilience of key Defense Critical Infrastructure in response to a combined physical and cyberspace attack.
3	Evaluate and examine the military's coordination process for providing cyber protection capabilities requested by civil authorities, including the ability to communicate and share information among the city, the private sector, and response partners.
4	Showcase the City of Houston as an emerging state and national leader in cyber incident response.

Table 2: JV 2.0 Research Objectives

JV 2.0 examined the possible effects of cyberspace attacks on a community's infrastructure and sought to identify how PPPs can enhance readiness and resilience. To do this, the exercise explored communication and collaboration methods among civic officials; city agencies; the private sector; and federal resource providers, such as the Federal Emergency Management Agency (FEMA) and the military.

By showcasing the City of Houston, the JV 2.0 exercise examined the existing incident response capabilities of both the city and Harris County, including how effective their coordination was across jurisdictions. The ACI looked at various aspects of coordination, such as how requests for support were made to federal organizations, such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation's (FBI's) Cyber Analysis Team, and DoD and National Guard Cyber Protection Teams.

Because the City of Houston recently endured Hurricane Harvey, it was an ideal testing ground for the objectives of JV 2.0. The city was interested in increasing visibility of the importance of the Greater Houston Region to the national economy, receiving federal funding to improve its cybersecurity, and highlighting the need for more resources. As an exercise participant, Houston received credit for conducting multiple types of exercises at one time from the Texas Division of Emergency Management and FEMA.

Figure 17: JV 2.0 TTX, Houston

Through JV 2.0, the ACI aimed to help state and regional civil officials better understand how to leverage DoD and National Guard cyber capabilities to protect public and private critical infrastructure. The exercise had two main objectives: to examine how DoD and National Guard cyber protection capabilities could be integrated into a domestic response when requested to do so by civil officials and to identify and prioritize research necessary for enhancing the Army's readiness to support civil officials and defend the homeland.

Figure 18: Lieutenant General (Ret.) Rhett Hernandez, U.S. Military Academy Cyber Chair, provides opening remarks at the JV 2.0 Legal Policy TTX in Fort Belvoir, Virginia.

At the conclusion of JV 2.0, the ACI was tasked with providing ARCYBER recommendations on developing cyber training objectives for the Army as well as for developing strategies and procedures to help large municipalities and critical infrastructure defend against cyberspace attacks. The exercise explored cybersecurity in ports and the integration of National Guard cyber protection assets into a domestic response to help ensure uninterrupted Army force projection.

2.5.2. JV 2.0 Timeline

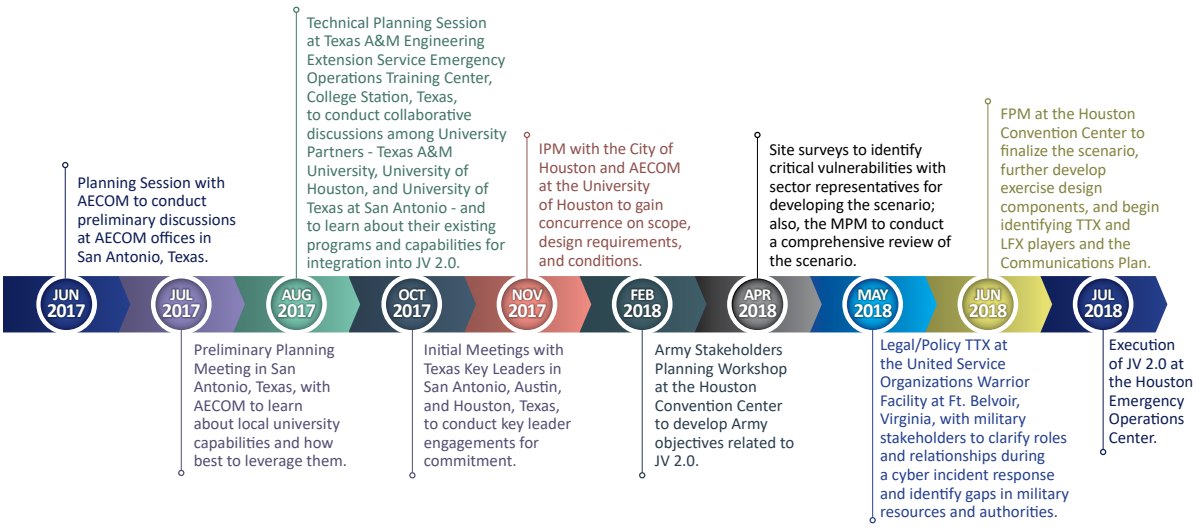

Figure 19: JV 2.0 Timeline

2.6. Lessons Learned

The ACI gleaned lessons from JV 1.0 and JV 2.0 that can help leaders at all levels improve their readiness for a major cyberspace attack.

Political and civil agency leadership must broaden their understanding of cyberspace from a static domain centered on IT and cybersecurity architecture and policies into a dynamic operational domain with adaptive adversaries. Accordingly, political and civil agency leaders should also have a broad range of knowledge about the basics of IT across agencies and sectors. A proper understanding of the ramifications of a cyberspace attack requires that knowledge of a given jurisdiction's IT department be shared regularly with the jurisdiction's executive staff. Such information sharing could take the form of advisory bodies, brown bag lunches, or quarterly exercises. Ensuring IT professionals can speak to executives in terms of business risks and impacts will help executives have a better understanding – if only at the strategic level – of the impacts of cyber threats and incidents on their operations. For example, before participating in a JV scenario, sectors with antiquated systems that may not be linked to Internet-based or cloud-based systems may have a false sense of security that they are not vulnerable to cyberspace attacks. While some risks are reduced in that situation, it is nevertheless important for the sectors to avoid complacency since there are other ways that they may be vulnerable.

Through the JV exercises, the ACI observed patterns across multiple sectors that could apply to any city or municipality. For example, during the first exercise, when operators and leadership met to discuss threats in their IT and business environments, they discovered significant and previously unknown linkages within their IT and OT systems.

The JV exercises illustrated the increasing interconnectedness and vulnerabilities of critical infrastructure sectors by bringing many key players to the same table and facilitating discussions about the threats to their IT and business environments.

Based on the exercises, the ACI recommends that cities revisit their network monitoring of all OT/SCADA systems to ensure only secure communications are allowed between production networks and the open Internet. Whenever possible, cities should mandate and enforce the use of data diodes or one-way network connections to monitor critical systems in real time and prevent the corruption of mission-critical data external to the sector. As more physical systems are operated, adjusted, regulated, monitored, or otherwise remotely accessed by computer systems, it is increasingly important to recognize that although this advancement may increase convenience and reduce costs, it also presents a growing potential attack surface for malicious actors.

Additional Lessons Learned:

- **Cyber fusion cells** are needed to improve public-private sector communication across a city or county (i.e., the local level, or the lowest level where coordination begins). This will enable cities to develop proactive defenses. Many states are currently developing cybersecurity strategies that include establishing ISAOs (see section 4 for additional information).[7] While there are existing means for enabling cyber preparation, prevention, and responses, cities must be able to communicate within the city as well as to state and federal authorities. As cities develop their cybersecurity plans, they should identify the organizations that are essential for the functioning of the city/county and consider developing PPPs aligned to their critical systems.
- **Cyber policies** must be developed at the city/county level in order to inform and shape state and federal policies. In particular, policies related to dealing with cyberspace attacks (e.g., ransomware) are needed imminently. Moreover, as these municipalities establish their policies, they should share them with other cities/counties.
- **City/county-level cyber exercises** provide opportunities for local levels of government to experiment in a safe and trusted environment. In an exercise setting, government actors can collaborate with their private sector partners to work through challenges, share best practices, and improve processes and procedures. In particular, cyber exercises provide ideal settings for the improvement of cities' and counties' readiness for preventing or responding to a cyberspace attack.
- **Communication with public and private entities** must be done in a timely manner. By engaging in exercises that simulate cyber incidents, municipalities can experiment alongside partners to develop innovative ways to share information outside of regulated and active investigations. Cities should address local, state, and federal information sharing challenges (e.g., computer forensics) associated with actionable information (e.g., law enforcement reporting). Exercises effectively enable this type of exploration that helps inform the public without compromising investigations.
- **Response processes that involve outside assistance** should identify industry partners and describe when and how they should be involved. As processes and procedures are developed, they should outline how they will be used to communicate to local, state, and federal information sharing centers.
- **Municipalities require communication plans** that follow formalized processes and efficiently counter the spread of misinformation during a cyberspace attack or outage. Municipalities should work with the private sector to quickly determine whether outages are cyber-related. Over time, this will reduce response time while more quickly informing state and federal policymakers.
- **Exploring the capabilities of Internet service providers (ISPs)** can help municipalities integrate the capabilities into the municipality response plans. For example, by working with ISPs, cities can develop plans to address denial of service attacks against 911 dispatch which could prevent the receipt of legitimate calls and severely slow emergency response times.
- **Operational and communication plans must be able to rapidly respond while avoiding the disclosure of sensitive information.** Response plans should outline ways of shaping the social media impact from a cyberspace attack that negatively affects electricity, transportation, or other infrastructure sectors.

2.7. Feedback

One of the primary goals of the JV exercise was to present agencies with the potential ramifications of a cyberspace attack and observe and judge the city's ability to respond.

The ACI conducted site surveys in conjunction with organizations from each of the participating critical infrastructure sectors. These surveys aimed to identify the policies and resources in place that could be used to respond to a combined physical and cyberspace attack. The ACI used the survey results to explore gaps in these policies and resources.

[7] Francesca Spidalieri, "State of the States on Cybersecurity," Pell Center for International Relations and Public Policy, Salve Regina University, November 2015, available from *https://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf.*

JV 2.0 requested feedback in the form of a site survey that asked participants the following 10 questions:

1. This question is about gaining a better understanding of a municipality's ability to respond to a multi-sector cyberspace attack. What does communication and information sharing look like at your organization and how does it communicate across?
2. This question is about gaining a better understanding of who should be a municipality's core team. During the initial response period (24-72 hours) of a cyberspace attack, what do you believe should be the public-private core team, and what is their role?
3. In your expert opinion, how SHOULD public-private sector agencies at the municipality level work through a cyber and physical attack?
4. In your expert opinion, what constitutes a cyber event in a municipality?
5. This question is about gaining a better understanding of learning or helping to identify the triggers that will cause the municipality to react during a cyber and physical event. In your expert opinion, what are the thresholds and escalation procedures during a cyberspace attack?
6. In your expert opinion, how does your organization know if an event is cyber-related? How do you validate indications of compromise?
7. In your expert opinion, what is your organization's messaging strategy to communicate to the public during an event?
8. How does a municipality leverage an ISP?
9. In the event that a cyberspace attack escalated to involve state-level assets (i.e., the National Guard), what do you believe would be the National Guard's response?
10. What are the capabilities needed?

We believe that the JV exercise series was the first of its kind to allow participants to drive the scenario on which they would be evaluated. This process enabled key stakeholders to focus on identifying weaknesses and crafting solutions for them. While these participants focused on their own priorities, the insights and data created during the exercise could be leveraged to better understand how the Army and DoD might be asked to support a "Cyber Worst Day" scenario. Over time, this research could even add to the growing literature about cyber exercises, their effectiveness, and their role in contributing to organizational and community learning. This process is critical to the theme of continuous learning and conducting after-action reviews that makes the Army and the DoD excel. The results of the JV 2.0 exercise can be used to request resources from state and federal agencies to help municipalities increase their resilience.

2.8. Methods of Data Collection and Analysis

The ACI and its partners developed a series of questions to gain an understanding of the actual consequences of a cyberspace attack. To collect and analyze data, JV used an application called Tracker that enabled observation of the Red and Blue LFX teams as the exercises unfolded. A chat portal allowed participants to communicate and record observations for future analysis.

2.9. The Future of JV

As interconnectedness continues to increase the potential attack surface for critical infrastructure, cities must increasingly incorporate risk mitigation considerations for cyber into their existing emergency response frameworks. As they currently exist, most are inadequate to adapt to the increasingly complex threat facing urban communities.

As municipalities become increasingly "smart cities" and Internet of things (IoT) devices increasingly control operational and physical systems, cyberspace presents new operational and safety risks for cities. Cities need to develop a bottom-up, integrated, risk management framework that is repeatable and adaptable to the rapidly evolving threats to urban communities. All levels of government need to think about how to address these risks within state and federal response plans.

Much like the Information Technology Infrastructure Library (ITIL), the JV framework serves as a playbook of modules that any municipality can use to exercise elements of its critical infrastructure. By focusing on its weaknesses and capabilities, enumerating dependencies and infrastructure partnerships, and better understanding the threat and response environments, cities can improve their preparedness. For example, a city with port operations, a public transportation system, a complex medical system, and a major tourism industry will look different from many other cities, but its vulnerabilities and dependencies among the sectors will have many similarities with other cities' vulnerabilities and dependencies.

In that sense, each city has its own constellation of infrastructure and related risks, but protecting such systems from cyberspace attack and responding to cyber incidents in them will have commonalities across significantly different cities.

The insights gained from activities like JV exercises can be leveraged to benefit other cities with similarities and used to help differentiate response options. The interdependencies among sectors introduce complexities that most other exercises do not explore or cannot simulate well. The JV research project attempted to analyze potential attack surfaces through an academic lens, thus increasing all U.S. cities' resilience. To be successful, the JV exercises need to change behaviors and the mindsets of the involved stakeholders in regard to cyberspace attacks.

3. OPERATIONAL FINDINGS AND RECOMMENDATIONS

The following paragraphs discuss key operational insights identified by researchers as a result of the JV project exercises.

3.1. Operational Risk Management

Growing physical and cyber risk to cities requires a different framework for risk mitigation due to a lack of consensus on the form that cities' frameworks should take, and because some currently utilized frameworks are inadequate to meet the changing and growing threat to urban communities. Most existing frameworks and approaches are designed for either asset-level or organization-level risk management. However, jurisdictions cross sectors, industries, disciplines, and organizations. For the Nation to defend itself, U.S. cities that are rendered vulnerable to an attack need an adaptable and scalable model to evolve the cybersecurity culture. A bottom-up approach is required to integrate an operational risk management system that is replicable and adaptive to the rapidly evolving threat to urban communities.

Cyberspace attacks can quickly overwhelm unprepared governments, in light of their limited resources. According to a 2016 cybersecurity survey, only 33 percent of local governments had a formal, written, cyber incident response plan (IRP).[8] Over the last few years, ransomware attacks have repeatedly targeted city and county governments and hindered their ability to perform services for the public. In addition to demonstrating a need for municipal governments to improve their cybersecurity practices, these attacks demonstrate a need for governments to build more resilience into their continuity and emergency response plans.

Prior to JV 2.0, the City of Houston consistently demonstrated its ability to respond to a diverse set of natural and man-made physical events. In 2017 alone, Houston successfully prepared and provided integrated emergency management services for the Super Bowl, Hurricane Harvey, and the World Series. The city, however, had never prepared for or faced a combined physical and cyberspace attack simulation. Additionally, although federal officials had exercised sophisticated, nation-state attacks on the homeland through exercises such as Cyber Storm, Cyber Flag, GRIDEX, and the FEMA National Level Exercise program, JV 2.0 was the first time that an exercise of this kind was driven from the local level. This effort required a considerable amount of relationship building, planning, and training prior to the event. JV 2.0 was a manpower-intensive activity designed to bring together and assess the readiness of participants at one point in time.

Implement Ongoing Education and Development Efforts

The JV approach can serve as a learning system and development effort. A series of JV exercises should be developed and educational workshops and conferences should be held in key cities and localities to identify vulnerabilities, develop solutions, propose actions, and share best practices.

Develop Risk Incident Response Campaign Plans

Statewide incident response campaigns should be developed, funded, and implemented to leverage the JV 2.0 model.

FEMA, DHS, the DoD, and the Department of Energy (DOE) should work together to develop a campaign plan to integrate the JV risk incident response model into the exercise framework at the national level (i.e., collaboratively among DHS, the DoD, and DOE). Military reserve component forces should be incorporated as part of this effort.

[8] ICMA, "Cybersecurity 2016 Survey – Summary Report of Survey Results," April 2017, available from *https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf.*

At the state level, funding and implementation may be aspirational for some states, but campaign plan development is comparatively low-cost. Numerous states offer examples, though they tend to be state-centric rather than focused on supporting local government and the public. Two such campaign plans are Michigan's Cyber Disruption Plan and West Virginia's Cybersecurity Workforce Strategic Plan, which specifically describe efforts to assist localities.[9]

Working with other state agency and community leaders, state emergency response coordinators should lead this effort and serve as the central resource for cities and localities in requesting assistance from state governments and the Federal Government. States, which play a critical role in supporting a city's response to cyberspace attacks, need to develop campaign plans for more scalable incident responses and more rapid information sharing. This includes disseminating information via traditional and social media, as well as combating false narratives.

Public affairs and public relations officials should immediately reach out to other counterparts to ensure messaging is synchronized across the board and that all members, parties, and organizations are tracking who is the lead and who is the release authority.

A public affairs strategy must be in place prior to a cyberspace attack with cascading effects that impact multiple sectors. This includes defining what information should be shared among various organizations responsible for crisis management and how public affairs officials and public relations agencies should coordinate to inform the public of events as they unfold. What information is appropriate to release to the public, when it should be released, and by whom it should be released are also important questions to address.

It is critical to have a shared understanding of the correct messages and products and who the release authority is for a real-world crisis to ensure that the responses are succinct and accurate, and that organizations are unified in releasing information to the public. There must be a clear understanding of who the lead is and how the other members, parties, and organizations can help support the lead. Public affairs and public relations officials need to create a shared list of important crisis points of contact (POCs). If synchronization does not occur prior to an incident, there will be information fratricide, and public perception and trust will deteriorate.

To achieve this synchronization, public affairs and public relations officials and counterparts should have at least one monthly synchronization meeting to discuss possible crisis scenarios to which all parties would need to respond until everything is agreed on by all parties.

Afterwards, quarterly or biannual meetings should suffice in which messaging, products, and sharing of information should be developed.

States should develop templates of press releases, products, and broad messaging (see appendix C) that can be tailored later to specific events. These templates should be collaboratively created, agreed upon, and shared by all parties. Spokespersons for each party involved should be nominated and chosen prior to events so that everyone knows who will be the spokespersons for specific crises.

Public affairs and public relations officials should agree on a tentative timeline for appropriate releases and have a plan in place regarding the different communication media through which information will be released during a crisis communication scenario. For example, if all electricity is turned off, does the communications team have enough batteries and sufficient signal to release information? What happens if cell towers go down? What is the backup to the backup? How will information be shared if everything goes analog for a while?

Develop Scaling Technology

Identified agencies should help develop technology offerings that enable the scaling of the JV 2.0 LFX component in support of NDAA, Section 1649, "Pilot Program on Modeling and Simulation in Support of Military Homeland Defense Operations in Connection with Cyber Attacks on Critical Infrastructure" (see appendix D).[10] They should not do this in isolation, but with meaningful input from localities. One of the reasons that the JV exercises succeeded, and that some similar efforts did not, is that they were

[9] National Governors Association, "Meet the Threat: States Confront the Cyber Challenge – Memo on State Cybersecurity Strategies," 2016, available from *https://ci.nga.org/files/live/sites/ci/files/1617/docs/1703CybersecurityStrategies.pdf.*

[10] National Defense Authorization Act of 2018, Pub. Law No. 115-91, § 1649 (2018).

developed in concert with the end users, rather than being tested on them. As mentioned earlier, the NDAA includes a provision for the development of a pilot program based on the lessons learned from the JV exercises.

The survey results for the LFX portion of the exercise were overwhelmingly supportive. Those who had contact with the cyber range wanted more time with the platform. However, the cost per license for access to cyber ranges was a cost-prohibitive factor for the research project as funded.

During a response to a cyber-related incident, there will be an increased need for forensic analysts to conduct the post-analysis. Degrees of sophistication vary; most organizations have some ability to ingest cyber intelligence information and some capacity to respond to or address cyber events that occur on their networks. However, these efforts generally lack the capability to analyze such events for the express purpose of generating actionable indicators of compromise (IOCs) that can then be shared with the larger community. Ideally this process would occur while a cyberspace attack was ongoing, but, at the least, it should occur after an incident has been resolved. Moreover, an organization would need to have in place sufficient skill sets, policies, procedures, and legal agreements to engage as an active and reliable participant in the generation of actionable intelligence that is useful to the larger community, rather than merely ingesting intelligence information from a regional sharing authority, such as a fusion center.

Seek Research and Development Support

Part of the challenge is identifying and applying for state and federal funds. States, cities, and localities should seek R&D support from the Executive Branch and Congress to develop appropriate systemic approaches to cybersecurity. There was a real, albeit stilled, influx of resources – both grant funding and technical expertise and support – to build counter-terrorism; intelligence; chemical, biological, radiological, nuclear, and explosives; and other capabilities at the state and local level following 9/11. There has been nothing similar as we have entered the era of cyber crises. There is a systematic challenge regarding bottom-up requirements and top-level funding. Cities may have the solutions, but they lack the federal funding for operations, remediation, and R&D.

Programs such as the Pentagon's Defense Innovation Unit, the Army Futures Command, and FEMA's Hazard Mitigation Grant program should be leveraged to help build the necessary support.

Evolve Public-Private Partnership Integration and Information Sharing

The private sector, which is affected by sophisticated, adversarial cyber threats, has the incentive and the capability to cooperate with the public sector to inform, develop, and provide solutions. City and local cybersecurity efforts should better integrate the private sector, particularly its critical infrastructure (e.g., electric grid, telecommunications, water, and transportation). PPPs should evolve (i.e., move beyond service-level agreements) to induce a cultural change for building trusted relationships, sharing information, and working together. In addition to partnerships with private sector companies, the role of non-profits in cybersecurity is extremely important.

From ISACs to ISAOs to federally-funded R&D centers to universities, cities and states have a large number of potential partners that want to contribute to the increasing security and safety of the digital world and the physical one that increasingly relies on it. For example, Texas, through the University of Texas at San Antonio (UTSA), is developing a cross-community, cross-sector ISAO for the state. The military should explore ways to assist states by growing their ISAOs and thereby supporting cross-sector information sharing and campaign planning and execution in accordance with Executive Order 13691.[11]

Considerations should also include the leveraging of best practices and lessons learned from the financial sector's Financial Systemic Analysis & Resilience Center (FSARC) to implement a similar model at local and state levels and, over time, the integration of municipalities into the intelligence community's processes. Additionally, the role of non-profits in cybersecurity is extremely important.

---

[11] *Executive Order 13691, "Promoting Private Sector Cybersecurity Information Sharing,"* Washington, DC: The White House, February 13, 2015, available from *https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.*

Lastly, key private sector representatives across all infrastructures should meet at least monthly in a single group to receive the same information and to understand the appropriate context. Additionally, private sector "certified active defenders" should be identified who have significant cybersecurity capabilities and can work under government authorization to help prepare for and respond to adversarial cyber threats.

Focus on Resilience Improvements

JV 2.0 provided additional lessons learned for further education and applied research. It highlighted the complexity of planning and executing a major urban incident response research project and pointed to the need for rapidly improving the cyber resilience of cities on which the Army and DoD depend when executing military missions, such as force projection. Resilience improvements must include more extensive public awareness, education, and applied research efforts. This type of activity would require the sustained engagement of senior Army and DoD cyber leadership.

3.2. U.S. Infrastructure Vulnerability

The U.S. military and its allies depend on civil and commercial infrastructure in and around cities. U.S. infrastructure requires greater protection due to its vulnerability to sophisticated physical and cyberspace attacks.

While military installations have internal critical infrastructure providers, they rely on service delivery from outside the installations' boundaries. For example, electrical service is delivered through commercial providers to the installation, where it is distributed by the internal utility company. In the event that a commercial provider was not able to supply electricity, an installation could run on backup power only for a finite period, and would generally do so at a diminished capacity.[12]

An integral participant in JV 2.0 was the SDDC battalion at Beaumont, Texas, a city on the state's coastal plain. Because of the large volume of cargo shipped from ports located along the U.S. Gulf Coast, these ports serve as major DoD transportation nodes for the overseas deployment of Army cargo. Two of these nodes are strategic ports located in Texas—the Port of Beaumont and the Port of Corpus Christi. Almost 40 percent of Army cargo deployed in support of Operation Iraqi Freedom flowed through these two ports. The Port of Beaumont is home to one of SDDC's port-handling battalions.[13]

Like the City of Houston, the Military Port of Beaumont is well prepared for natural hazards and physical threat events. However, JV 2.0 highlighted the challenges the port faces in preparing for and responding to a physical or cyberspace attack. The project identified gaps in service-level agreements, understanding of cyber threats, and overall cyber response procedures.

This requires cross-talk with owners of critical infrastructure in accordance with the National Infrastructure Protection Plan and the Critical Infrastructure Partnership Advisory Council to discuss priorities of effort within resilience response.[14] In the absence of guidance, the energy grid will default to restoring the most populous areas, which are not likely to be military installations. Installation commanders should ensure that utility companies recognize the importance of service being restored as quickly as possible based on mission requirements.

The Defense Support of Civil Authorities (DSCA) process has been well established, while Defense Support to Cyber Incident Response (DSCIR) within the DSCA framework is still being developed. Authorities and the consent-based nature of assistance are very different between DSCA and DSCIR. There is a significant difference between responding to a request from local civil authorities for disaster response and responding to a lead federal agency (LFA) that is responding to a request for assistance from a private entity. In the cyber incident response, the LFA responds within the limits of its agreement with the private entity.

---

[12] Aaron Mehta, "Pentagon Weighs New Requirements to Secure Military's Vulnerable Power Grid," *Defense News*, November 29, 2017, available from *https://www.defensenews.com/pentagon/2017/11/29/pentagon-weighs-new-requirements-to-secure-militarys-vulnerable-power-grid/.*

[13] Department of the Army, "Moving the Army Texas Style," *Army Logistician*, July-August 2004, available from *https://alu.army.mil/alog/issues/julaug04/texas.html.*

[14] Department of Homeland Security, "Critical Infrastructure Partnership Advisory Council," updated March 29, 2019, available from *https://www.dhs.gov/critical-infrastructure-partnership-advisory-council.*

Improve Transportation and Maritime Security

The Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff, and related Combatant Commands should develop an operational risk management framework that better enables the protection of critical force projection elements inside and outside of military boundaries for defense surface deployment and distribution. Collaboration and planning must include the Military Reserve, the National Guard, DHS, and DOE.

U.S. Transportation Command is already held to certain DoD cybersecurity requirements. Per DoD Instruction Memo 8510.01, "Risk Management Framework," the DoD adheres to the National Institute of Standards and Technology (NIST) framework.[15] However, some commercial partners may not be held to these same standards and, as such, the risks associated with these vulnerabilities can be further exacerbated during coordinated response efforts.[16] DoD contractors and subcontractors are also subject to additional cybersecurity measures. The Defense Federal Acquisition Regulation Supplement requires NIST SP 800-171 compliance for all of these entities in order to ensure better protections for Controlled Unclassified Information residing in nonfederal systems.[17]

The application of these same standards and other available NIST risk management tools could act as a starting point at the state and local levels of governance to more robustly protect both federal and nonfederal deployment and distribution operations during cyber emergencies.[18] The City of Houston already maintains a repository of this information within its own Cybersecurity Control Implementation Interface (CCII), which provides access to various NIST frameworks, policy and procedure "boilerplates," and other interactive utilities.[19] The 2018 National Cyber Strategy highlights the prioritization of transportation and maritime cybersecurity; this includes a focus on clarifying roles, identifying specific responsibilities, enhancing mechanisms for international coordination, and developing "next-generation cyber-resilient maritime infrastructure."[20] The 2018 DoD Cyber Strategy echoes this sentiment as well with the specific objective of defending both DoD and non-DoD critical infrastructure, systems, and networks against malicious activity.[21]

Accordingly, national recognition and prioritization of maritime transportation, deployment, and distribution capabilities can further enable the allocation of resources at state and local levels of governance to better secure these functionalities during cyber emergencies. To accomplish this, state and local levels of governance can take the lead with federally provided resources to implement these critical civilian maritime and transportation requirements within their areas of responsibility. Identified agencies should further assess the cyber resilience and readiness of global military transportation units, such as SDDC.

Work with NATO and Allies

Because other countries may possess authorities at the tactical level and may be able to employ

---

[15] Joey Cheng, "DOD Switches to NIST Security Standards," *Defense Systems*, April 3, 2014, available from *https://defensesystems.com/articles/2014/04/03/dod-adopts-nist-security-standards.aspx.*

[16] Scott Maucione, "TRANSCOM Worried About Cybersecurity Gap Between DoD and Civilian Networks," *Federal News Network*, March 30, 2017, available from *https://federalnewsnetwork.com/cybersecurity/2017/03/transcom-worried-cybersecurity-gap-dod-civilian-networks/.*

[17] National Institute of Standards and Technology, "DFARS Cybersecurity Requirements," U.S. Department of Commerce, updated June 28, 2018, available from *https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance.*

[18] National Institute of Standards and Technology, "Cyber Risk Management," U.S. Department of Commerce, updated October 17, 2018, available from *https://www.nist.gov/mep/cybersecurity-resources-manufacturers/cyber-risk-management.*

[19] City of Houston, "Cybersecurity Control Implementation Interface," available from *https://www.cciitool.info/splash.*

[20] Office of the President of the United States, "National Cyber Strategy of the United States of America," Washington, DC: The White House, September 2018, available from *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.*

[21] U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy," Washington, DC: U.S. Department of Defense, 2018, available from *https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF*

resources more quickly, the U.S. military should work with allies to develop similar integrated protection frameworks in transload forwarding areas abroad and with front-line states using mutual aid, Status of Forces Agreements, and Acquisition and Cross-Servicing Agreements. As a starting place, these efforts should be developed within NATO through the fostering of support networks. Additionally, identified agencies should develop and conduct Theater Support Cooperation Plan activities to help allied armies and military forces develop similar integrated protection frameworks in transload forwarding areas and with front-line states.

There are a number of international frameworks and agreements that may act as appropriate mechanisms for integrated allied protection. The NATO Industry Cyber Partnership (NICP) is such an allied framework that remains focused on cooperation with the private sector for network protection, implementation of risk reduction standards, international and national data protection, and additional partnerships with both national academia and scientific institutes involved in cyber defense capabilities or capacity building.[22] NICPs build upon preexistent structures and relationships among member nations – specifically, Computer Emergency Response Teams, NATO industry representatives, and relevant vectors within academia – in order to ensure "efficient and adequate support" during cyber emergencies or incidents.[23] Accordingly, this existing NATO framework creates an opportunity for further synchronization and protection of forward operating areas during domestic or even international cyber emergencies. The NATO Cooperative Cyber Defense Centre of Excellence conducts research and training in cyber defense, to include Locked Shields and Crossed Swords, improving readiness and cooperation among NATO members.[24]

The European Union (EU) also recently agreed to create a common framework that may support additional international cooperation and integration efforts during cyber emergency response efforts. The EU Agency for Network and Information Security (ENISA) is the primary agency that has been designated to support implementation of the EU's Cybersecurity Act, which focuses on certification of "specific ICT [information and communications technology] processes, products, and services."[25] Although currently considered to be preliminary, early coordination efforts can help synchronize acquisition-specific agreements to positively impact protection efforts during various cyber incidents or emergencies. Additionally, ENISA heavily focuses on PPPs through the European PPP Resilience effort in order to address Critical Information Infrastructure Protection; the 2013 European Cybersecurity Strategy and the Network and Information Security Directive of 2016 further support these efforts, as would the proposed EU Cybersecurity Act.[26]

Lastly, the Group of Seven (G7) also offers an additional framework that can support an integrated approach to protection efforts during cyber events. The G7's Principles and Actions on Cyber emphasizes support for "decisive and robust measures" against malicious cyber activities, promoting cooperation and collaboration among businesses, research institutes, and nations regarding both international and national cybersecurity efforts.[27] G7 member nations may be able to initiate specific actions through their own protection frameworks, which could support a more unified operational support structure during domestic cyber emergencies or incidents.

---

[22] NATO Communications and Information Agency, "NATO Industry Cyber Partnership (NICP)," North Atlantic Treaty Organization, available from *https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx.*

[23] Ibid.

[24] "NATO Cooperative Cyber Defense Centre of Excellence," NATO Cooperative Cyber Defense Centre of Excellence Website, n.d., available from *https://ccdcoe.org/.*

[25] General Secretariat of the Council, "EU to Create a Common Cybersecurity Certification Framework and Beef Up its Agency – Council Agrees its Position," Council of the European Union, June 8, 2018, available from *https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/.*

[26] European Union Agency for Network and Information Security, "National Cyber Security Strategies," European Union, available from *https://www.enisa.europa.eu/topics/national-cyber-security-strategies.*

[27] Group of Seven, "G7 Principles and Actions on Cyber," U.S. Department of State Website, March 13, 2016, available from *https://2009-2017.state.gov/s/cyberissues/releasesandremarks/258028.htm.*

3.3. Cyber Response Processes and Capabilities Assessment

National Guard units are providing physical security to support cities and developing cyber capability to provide cyber protection. State military departments are working to evolve cyber response processes, including partnership strategies, and capabilities more rapidly to help cities. As capabilities are developed, they need to be inventoried and regularly assessed for readiness and employment inside and outside of state jurisdictions. Mission assignment and authorities are given for a limited duration.

JV 2.0 included discussions and observer participation with a variety of Reserve and National Guard units, including the Army Reserve, the Michigan Department of Military and Veterans Affairs, the Washington State Military Department, and the Texas Military Department. These interactions demonstrated that state National Guards have significant physical response capabilities with well documented and practiced procedures. State National Guard units are developing cybersecurity capabilities and capacity at varying levels, but these capabilities are not yet being employed in support of scenarios like JV 2.0. Processes for more rapidly developing and deploying state National Guard cyber capabilities need to be developed and exercised as part of homeland defense campaign plans.

Develop a Cyber Asset Inventory

Previous exercises tended to gloss over how personnel are transitioned from one status to another and whether DHS has much interest in those transitions. The DoD should develop and maintain an inventory of existing and emerging, critical, National Guard and Reserve, cyber capabilities. This inventory could be leveraged by state military departments, enabling better coordination between the DoD and DHS. These capabilities should be tracked as they are developed.

States need to develop and publicize their concepts of operation, including training and equipping, apart from Title 10 efforts to train and equip Cyber Protection Teams. Many reservists and Guardsmen serve in a spectrum of civilian jobs, but it is critical that they understand their roles when mobilized in their military capacity, whether Title 10, Title 32, or State Active Duty (SAD). The Posse Comitatus Act (PCA) does not apply to Title 32 or SAD.[28] Worthy of additional consideration are the provisions of both the Stafford Disaster Relief and Emergency Assistance Act and the Economy Act, which must be addressed up front.[29, 30]

With the exception of training exercises, DSCA; DSCIR; National Guard Civil Support; Domestic Operations; and FEMA's National Disaster Recovery Framework, codified in 2011, would be mobilized for a specific event. In designing future JVs, the disconnect between response to cyber incidents in a SAD capacity, most likely as part of a Defensive Cyberspace Operations Element (DCOE), and the response of National Guard personnel integrated into a Title 10 response in support of an LFA should be examined.

The Major General Tim Lowenberg National Guard Cyber Defenders Act has been proposed to create "National Guard Cyber Civil Support Teams" that serve at the discretion of state governors. If passed, this legislation may provide a mechanism and funding for assisting local authorities in establishing these teams to bridge federal and nonfederal response efforts during cyber emergencies or disasters.[31] This could address those factors in a particular scenario that would drive a decision to use SAD personnel versus integrating with the DoD response. These units can act as an important link to private sector entities, as many of these individuals gain critical skills, training, and experience from their regular civilian employment capacity that can be leveraged during federal, state, or local cyber emergencies.[32] Efforts also continue to effectively align National Guard cyber capabilities with all 10 FEMA regions by fiscal year 2022 in order to ensure adequate emergency coverage; this coverage is projected to include 10 directly-aligned Cyber

---

[28] Posse Comitatus Act of 1878, 18 U.S.C. § 1385 (1878).
[29] Stafford Disaster Relief and Emergency Assistance Act of 1988, Pub. Law No. 100-707 (1988).
[30] Economy Act of 1933, 38 U.S.C. § 701 (1933).
[31] Major General Tim Lowenberg National Guard Cyber Defenders Act of 2018, S. 2887, 115th Congress (2018).
[32] Isaac R. Porsche III, Caolionn O'Connell, John S. Davis II, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur, *Cyber Power Potential of the Army's Reserve Component*, Santa Monica, CA: RAND Corporation, 2017, available from *https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1490/RAND_RR1490.pdf.*

Protection Teams, one per region.[33] These teams will be in addition to five Cyber Support Companies and five Cyber Warfare Companies, all operating under state authorities.[34]

Cities and municipalities should analyze the potential costs, appropriateness, readiness, risk, lethality, and legality[35] of potential responses to a cyberspace attack to better understand in what ways the National Guard and Reserves might be needed to assist. In particular, they should consider:

- Who will be paying or reimbursing the Guard or Reserves?
- When is a request for military forces considered an appropriate response?
- Does the request for support impact the National Guard's and Reserves' performance of the primary mission?
- How can the safety of forces be assured?
- What is the public relations risk of acting or not acting?
- What should the rules of engagement for military forces be?
- Does the need to restore cyber capabilities save lives, prevent human suffering, or mitigate great property damage?

3.4. The Role of States in Cyber Incident Response

States play a critical role in supporting city responses to physical and cyber events. States must develop campaign plans for more scalable incident responses and rapid information sharing. Several states are in the process of establishing fusion centers and ISAOs. As an example, the State of Connecticut issued the Connecticut Cybersecurity Strategy in 2017 and the Cybersecurity Action Plan in 2018. The plan includes sections for state government, municipal governments, business, higher education, and law enforcement to address the following goals: cyber literacy, preparation, response, recovery, communications, and verification.[36]

Texas represents another example. With the support of the Texas Governor's Office, JV 2.0 participation included the Texas Department of Public Safety (DPS), the Directorate of Information Resources (DIR), and the Texas Military Department. DIR and DPS were active participants throughout all phases of JV 2.0. Importantly, state universities, such as the University of Houston, UTSA, and Texas A&M University have a special relationship with the state and played a critical role in furthering education and application in JV 2.0. Lessons learned at the state level included the need for cyber resources to be more integrated into state emergency response activities.

States must provide leadership and direction as well as coordinate the necessary funding to enable cities to better protect at-risk infrastructure and services. Municipalities must incorporate infrastructure sectors into their emergency response plans to help mitigate and respond to the threats they face in both the physical and digital domains. Information sharing programs are necessary but not sufficient. States need to develop and sustain integrated incident response exercise and training programs which include government, industry, and academic partners.

This is important to view in the context of many states struggling to secure their own networks or to resource and staff their cybersecurity organizations. The provision of additional support by states to localities, particularly of the operational and tactical variety, is probably aspirational in the immediate term. Some states are experimenting with models that provide such support, but, in many cases, they are either functionally narrow (like providing a vulnerability scanning or penetration testing capability) or in their organizational infancy.

Adoption by States and Municipalities

Given the array of current threats to major cities, a primary goal of JV was to build a framework that could be replicated in any city. In the future, determined or unscrupulous attackers will likely continue to target and overwhelm local and state

---

[33] National Guard Bureau, "NG Cyber Defense Team," United States National Guard, updated December 2017, available from *https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/NG%20Cyber%20Defense%20Team%20Fact%20Sheet%20(Dec.%202017).pdf.*

[34] Ibid.

[35] Federal Emergency Management Agency Emergency Management Institute, "IS-75: Military Resources in Emergency Management," presentation, n.d., available from *https://training.fema.gov/emiweb/is/is75/visuals/visuals%20-%20powerpoint.pptx.*

[36] State of Connecticut, "Cybersecurity Action Plan," May 2, 2018, available from *https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en*

governments unless they adopt better cybersecurity practices and response procedures. Even then, the prognosis is complicated. Cities and states often have far smaller IT budgets and staffs than their federal partners or private sector companies do, and these better-resourced and better-staffed organizations continue to experience cybersecurity problems.

A coordinated attack could overwhelm available federal and state cyber resources. This potential for disaster requires cities to maintain internal cyber capabilities; remain proactive in cybersecurity; incorporate cyber incident response measures into their disaster recovery and response procedures; and, in some cases, maintain the capacity to continue certain mission-critical functions without computer assistance or support.

Due to population density and the density of infrastructure and the man-made environment, cities are particularly susceptible to cyber threats that can quickly spread from one network to the next and one sector to the next and become kinetic – that is, they can spread from information processing systems through cyber-physical systems to cause real-world service interruptions and even risk safety and lives. A power disruption can impact traffic on subways, stranding thousands of people for prolonged periods of time. Compromised technological systems can have devastating effects on the healthcare sector, as modern medical centers have a tremendous and growing reliance on technology to control and program medical devices like pacemakers, which are implanted in people's bodies.

A rapid proliferation of cyberspace attacks can quickly overwhelm unprepared governments. In February and March 2018, ransomware attacks had serious impacts on online services in Atlanta, Georgia; 911 dispatch services in Baltimore, Maryland; and government networks in Davidson County, North Carolina.[37] Recovering from the attacks could cost Atlanta and its taxpayers as much as $17 million.[38] These attacks serve as real-world examples of the types of serious threats that U.S. cities face and the need for states and municipalities to act now to develop and implement effective cybersecurity strategies.

The State of Connecticut has approached cybersecurity in a manner consistent with the ACI's recommendations and could serve as a model for other states or even large cities. In July 2017, the state issued the Connecticut Cybersecurity Strategy and followed it up in May 2018 with a Cybersecurity Action Plan. This plan includes sections for state governments, municipal governments, businesses, institutions of higher education, and law enforcement to address the following goals: cyber literacy, preparation, response, recovery, communications, and verification. Additionally, the plan identifies priorities and action steps while addressing legislative, regulatory, and budgetary considerations.[39] Since the Greater Houston area is roughly the size of Connecticut and twice as populous, it would not be a stretch for the local government to also develop and implement a strategic vision.

A model such as Connecticut's is a great step in the right direction. Its success, however, will still largely rely on proactive municipal governments developing, implementing, and testing their own plans as well as legislators providing input with a long-term outlook on security.

The organization and structure of Los Angeles's Cyber Intrusion Command Center and LA Cyber Lab, as well as the New York City Cyber Command, can serve as models for large cities that are trying to balance their business and security concerns while improving preparedness and coordinating responses.

Develop a Common Communication Protocol

As recently experienced, regularly occurring events, such as elections, can be manipulated. Robust interagency involvement staffed with the appropriate authorities can support the monitoring of the actions of threat actors in urban environments. Municipalities within jurisdictions must develop a way to come together in the wake of a major emergency, whether it is a major healthcare catastrophe like a pandemic or a cyberspace attack that targets major infrastructure and endangers the public. At the municipality and county level, there is a need to establish a common protocol. A jurisdiction should be judged on its ability to operate under a common set of principles

[37] Kate Brumback, "Cyberattacks Wakeup Call for Local Governments to Prepare," *Associated Press*, March 30, 2018, available from *https://www.apnews.com/1c599d36222544e1928e07b62bd9b713.*

[38] Stephen Deere, "Confidential Report: Atlanta's Cyber Attack Could Cost Taxpayers $17 million," *The Atlanta Journal-Constitution*, August 1, 2018, available from *https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/?icmp=np_inform_variation-control.*

[39] State of Connecticut, op. cit.

that all component departments and agencies are aware of in any given emergency. A critical event will raise a variety of implications for the various sectors involved; as the adage goes, where you stand depends on where you sit. Cities, counties, and states coordinate and interact differently across the country. While there is no one-size-fits-all model of this kind of coordination, the move in a general direction to improve interoperability and information sharing is an important one. There are ongoing efforts today that exist at the federal level to evolve these efforts. The two examples known are practiced within the financial and energy sectors.

In 2016, eight U.S. banks from the Financial Services Information Sharing and Analysis Center (FS-ISAC), an organization created in 1999 by the financial services sector to address emerging physical and cybersecurity threats, began working together to study ways in which the critical infrastructure of the Nation's financial system could be made more robust and its systemic risks reduced. This effort led to the establishment of the FSARC, a partnership of participating banks; industry members; and U.S. Government agencies, such as the Department of the Treasury (TREAS), DHS, and the FBI. The FSARC identifies, assesses, and oversees efforts to mitigate systemic risks to the Nation's financial system presented by the threat of cyberspace attacks.

With the initiatives of the FS-ISAC, the financial services sector became the first CIKR sector to begin evolving the way that a sector-specific agency exchanges information. This best practice within the financial sector is exploring cross-communication among other priority sectors – power, utility, and telecommunications – which is driving a new model of information sharing to the next generation. This model of public-private collaboration provides a level of realization that there are dependencies, and understanding how information exchanges is critical. Project Indigo, a pilot program recently developed by FS-ISAC and U.S. Cyber Command (USCYBERCOM), represents a good example of an information sharing channel designed to provide data to USCYBERCOM, DHS, and TREAS about nation-state hacking aimed at the financial sector.[40]

Within the emergency services sector, law enforcement typically has the earliest situational awareness during a critical event. It is common for law enforcement to not immediately disclose this information so as to not damage the investigation of what could become a criminal case. This approach can adversely affect sectors like healthcare that have a different set of concerns, such as patient care. Critical questions include the following:

- At what point can IOCs be shared between law enforcement and the technical staff and chief information officer (CIO) of each sector?
- How can this information sharing be maximized for the safety of healthcare patients or other sectors' stakeholders and the public at large without the potential of damage to an ongoing or future criminal case?

These are difficult questions to answer, but balancing the factors they present is critical, and a jurisdiction will be judged by the court of public opinion no matter how the decisions are made.

3.5. Policy and Legal Authorities

Policy and legal authorities at the federal and state levels currently do not sufficiently empower cities to respond to cyber incidents. Policies and authorities need to be reviewed and adjusted to better help cities defend against sophisticated physical and cyber threats. Currently, the exploration of cyber mutual assistance is practiced only within the energy sector.

A key element of JV 2.0 was a military policy and legal workshop held prior to the TTX. The TTX allowed stakeholders to create a baseline where, before issues arose in exercise execution, experienced personnel across the various sectors identified key issues and inadequacies in the current DSCA for cyber incident response and in the policies and procedures for providing cyber mutual assistance through National Guard and industry sectors across state lines. The workshop also noted the lack of an operational net assessment process at the national level for continuously assessing comprehensive physical and cyber risks to cities and military installations.

[40] Chris Bing, "Inside 'Project Indigo,' the Quiet Info-Sharing Program between Banks and U.S. Cyber Command," *CyberScoop*, May 21, 2018, available from *https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/*.

Develop Cyber Response Procedures

Identified agencies should work with the National Guard and others to develop cyber response procedural handbooks to be shared across state military departments. The National Guard should be trained on cyber response policies and procedures, and the effectiveness of exercise programs used by U.S. Northern Command, USCYBERCOM, and FEMA should be assessed.

NIST offers an incident response framework – the NIST Computer Security Incident Handling Guide – that provides assistance in the creation of an effective and efficient incident response methodology.[41] The framework has been applied at the federal level, and could potentially be adopted at both the state and local levels as well, provided it can be appropriately scaled to state and local governance architectures. As previously mentioned, the City of Houston already maintains a repository of this information within its own CCII.[42]

Another resource worthy of attention is the DHS Critical Infrastructure Cyber Community Voluntary Program, which provides technical assistance in the application of the NIST framework for state, local, tribal, and territorial governments.[43] The coupling of information that is readily available via Houston's CCII, along with DHS technical implementation support via the United States Computer Emergency Readiness Team, could better enable the application of a more scalable cyber response framework at local levels of governance.

In addition to federal support mechanisms, other model municipal and regional architectures could also potentially be applied to cyber response procedures, such as San Diego's Region-Wide Incident Response Guide. This guide provides a framework that both incorporates and synchronizes private and public sector cyber emergency response efforts.[44]

The State of California also has a cyber incident response guide that can provide context for the formulation of a regional or municipal model. Created by the California Office of Emergency Services, this plan provides guidance for the creation of specific IRPs that are directly nested in the state's Cybersecurity Integration Center and that focus on reducing the severity of cyber incidents.[45] Therefore, other existing federal, state, and regional cyber incident response guides can also provide a mechanism for the creation of such a guide at the city level.

Lastly, the Army Reserve's Immediate Response Authority (IRA)[46], which has never been exercised for cyber, should be considered.

Develop Cyber Mutual Assistance Policy and Implementation Guidance with Ongoing Intelligence Assessment

Military organizations such as the National Guard Bureau should explore possibilities in cyber mutual assistance practice. This would involve developing policy and associated implementation guidance to enable more proactive and sustained, national military support to cities and localities defending against physical and cyberspace attacks.

Local communities and state and national security leaders should develop and annually update national intelligence assessments of the physical and cyber capabilities of designated nation-state and terrorist

---

[41] Paul Chichonski, Tom Millar, Tim Grance, and Karen Scarfone, *NIST Special Publication 800-61: Computer Security Incident Handling Guide, Revision 2*, Gaithersburg, MD: U.S. Department of Commerce, August 2012, available from *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.*

[42] City of Houston, op. cit.

[43] United States Computer Emergency Readiness Team, "Critical Infrastructure Cyber Community Voluntary Program," U.S. Department of Homeland Security, available from *https://www.us-cert.gov/ccubedvp.*

[44] San Diego Cyber Center of Excellence, *San Diego Region-Wide Cyber Incident Response Guide*, City of San Diego, October 2017, available from *https://sdccoe.org/wp-content/uploads/2017/10/San-Diego-Cyber-Incident-Response-Guide-10-17.pdf.*

[45] California Cyber Security Integration Center, *California Joint Cyber Incident Response Guide*, California Office of Emergency Services, February 27, 2018, available from *https://www.caloes.ca.gov/LawEnforcementSite/Documents/California-Joint%20Cyber%20Incident%20Response%20Guide.pdf.*

[46] *DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)*," Washington, DC: U.S. Department of Defense, December 29, 2010, available from *https://www.dco.uscg.mil/Portals/9/CG-5R/nsarc/DoDD%203025.18%20Defense%20Support%20of%20Civil%20Authorities.pdf.*

adversaries to exploit predictable natural and threat-based, man-made events. The newly-created DHS National Risk Management Center and the Cybersecurity and Infrastructure Security Agency should also be engaged.

Identified military organizations should assist OSD and interagency partners, such as the new DHS National Risk Management Center, in the development of a continuous net assessment process for the Federal Government that can help municipal and military installation leaders achieve a better understanding of physical and cyberspace threats and risks to their enterprises. The DHS National Risk Management Center was created to improve the ability of the private sector and the Federal Government to work together to combat adversaries, citing nation-state threats to private industry.[47]

Review and Improve DSCA Procedures

Associated organizations should continue to review DSCA procedures in light of JV 2.0 findings and develop recommendations for providing Army and military commander IRA in cyberspace.

Create a Legal Framework

Because cyber effects can influence the ability of state and local authorities to react, legal frameworks should be developed that address responses to cyberspace attacks that occur simultaneously with a physical attack. DSCA is the process by which DoD personnel and assets are used to assist in missions typically undertaken by civil authorities, such as responses to natural and man-made disasters, law enforcement support, special event support, and other domestic activities. DSCA is well established as an all-of-nation/whole community approach, integrating efforts across federal, state, local, private sector, community, nongovernmental, and individual partners.

While DSCA is well established, the more specific DSCIR is still under development. At present, DTM 17-007, "Interim Policy and Guidance for Defense Support to Cyber Incident Response," provides temporary guidance until DSCA (DoDD 3025.18; Joint Publication 3-28) can be revised to include cyberspace attacks.[48, 49, 50]

It will be important to publicize and socialize any changes or emerging policies with states (which directly interact with federal coordinating officers and defense coordinating officers) and cities that typically do so through state representatives because, similar to traditional, non-cyber, DSCA operators, it is possible that lack of understanding of the policy, process, or requirements could result in unnecessary delay or confusion.

Transition to Law Enforcement

It is important for all responders to know when a response to a cyberspace attack transitions to law enforcement and who is responsible for preserving the forensic integrity of data and other evidence. This legal framework is critical because, whether the mission of an agency involves cyber operations, all federal assets and organizations need to understand the Request for Assistance and Emergency Management Assistance Compact (EMAC) processes before they preemptively (and unlawfully) insert themselves into incident response. In accordance with the National Incident Response Framework (Presidential Policy Directive 41), the DoD must understand that, regardless of its rank or seniority, it is not the lead during a cyberspace attack.[51] Rather, the role of the DoD is to support the local authorities, whether on-site or in a remote capacity. EMAC forces remain under the administrative control of respective states and operate at the direction

---

[47] Jim Finkle and Christopher Bing, "U.S. Seeks More Cooperation with Private Sector to Fight Cyber Attacks," *Insurance Journal*, August 1, 2018, available from *https://www.insurancejournal.com/news/national/2018/08/01/496636.htm.*

[48] Deputy Secretary of Defense, *Directive-Type Memorandum 17-007: Interim Policy and Guidance for Defense Support to Cyber Incident Response*, Washington, DC: Office of the Secretary of Defense, updated May 25, 2018, available from *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-007.pdf?ver=2018-05-25-080104-323.*

[49] *DoD Directive 3025.18*, op. cit.

[50] *Joint Publication 3-28, "Defense Support of Civil Authorities*," Washington, DC: Joint Chiefs of Staff, U.S. Department of Defense, October 29, 2018, available from *https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.*

[51] *Presidential Policy Directive 41, "United States Cyber Incident Coordination,"* Washington, DC: The White House, July 26, 2016, available from *https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.*

of the state's governor, adjutant general, or other designee. This requires a memorandum of agreement to memorialize the duties and responsibilities of the various organizations to ensure that C2 remains clear. Additionally, should the DoD act preemptively without the proper authorization, the DoD would face the financial risk under these circumstances that an organization will not pay for services that it did not request, need, or want, potentially running afoul of the Antideficiency Act by incurring financial obligations before they are authorized.[52]

Potential Legal Repercussions

Cybersecurity first responders should not be put in jeopardy of legal repercussions because of a request for their support at the scene of a cyberspace attack. In the DHS and FEMA context, DSCA is executed through pre-scripted mission assignments that are generally well understood. We are in the beginning stages of the cyber incident response context.

There is much work to do within the DoD and the National Guard to understand and shape the differences among responses of the National Guard under SAD, Title 32, and Title 10 authority. Previous exercises tended to gloss over how personnel are transitioned from one status to another and the degree to which DHS has interest in those transitions, which raises the question: What drives the decision to use SAD personnel versus integrating with the DoD response? Consider the differences in a potential response to cyber incidents in SAD capacity, most likely as part of a DCOE, and the response of National Guard personnel integrated into a Title 10 response in support of an LFA. The authorities, capabilities, and needs may not always exist at the same place and time or within the same organization; thus, thinking about the way that companies, jurisdictions, and the DoD leverage each other's capabilities is key in responding effectively to incidents without undermining democratic values, the public trust, or the rule of law.

The PCA limits the powers of the Federal Government to use federal military personnel to enforce domestic policies within the United States.[53] Neither active duty personnel nor reservists are authorized to conduct law enforcement, and must operate in accordance with the mission.[54] However, during the mission, some may encounter illegal or fraudulent activity, conduct law enforcement activities with the best of intentions, and ask for forgiveness later rather than permission beforehand. This is better understood in the DHS and FEMA context, but is still under development in the area of cyber incident response.

Normally, initiative is a positive attribute, but FEMA may not reimburse for preemptive work or work performed outside the scope of mission assignment. Those that operate outside of their mission command not only face potential disciplinary action, but also jeopardize relationships among the various stakeholders. For example, the Computer Fraud and Abuse Act criminalizes knowingly accessing "a protected computer" without authorization or beyond authorization, and thus jeopardizes relationships among the various stakeholders.[55]

This is an unexplored area because there have been relatively few large-scale cyber incident responses by states and cities – but episodes like those in Atlanta, Baltimore, and elsewhere suggest that one major set of questions moving forward will pertain to the authorities, liabilities, and responsibilities of various officials and levels of government in regard to data privacy or data protection issues arising from cyber incident response activities.

This raises a critical question: Why mobilize an active duty or reserve unit if it is prohibited from doing what is needed? If Service members get injured while performing an unauthorized service, subsequent line of duty determinations or workers' compensation claims become uncertain. In a traditional law enforcement setting, the Rules for the Use of Force by civil authority are established by federal law developed through many years of civil litigation involving the liability of the Federal Government for the actions of federal employees, including military personnel. States, as separate sovereigns, have their own tort liability laws that largely coordinate with the federal standards, but may have differences. Incidents are resolved quickly. As bad actors are generally visible, the rules on escalation of force are clear and the liability is predictable.

---

[52] Antideficiency Act of 1982, 31 U.S.C. § 1341 (1982).
[53] Posse Comitatus Act of 1878, op. cit.
[54] Ibid.
[55] Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (1984).

Conversely, with "Rules for the Use of Cyber," which has not been formally codified, attribution issues and effects are complicated and, therefore, serious questions arise, such as the following:

- How certain is attribution?
- How does one escalate in cyber?
- Who is the appropriate authority for approving a cyber response?
- What, if any, are the liability limitations?
- Should a response to a cyberspace attack be limited to or even involve a cyber-based response?
- What are possible second and third-order effects of a cyber-based response?

4. ACADEMIC FINDINGS AND RECOMMENDATIONS

JV is a research project that provides both operational and academic insights. While the operational element focuses on developing better answers, the academic element of JV focuses on how to ask better questions. The academic insights below address conducting gap analysis, coordination studies, scenario development, cyber education, organizational interaction and integration, and data collection. The following paragraphs discuss key academic insights identified by researchers through the JV project exercises to date.

4.1. Gaps in Cyber Incident Response

Although the JV project has helped make significant strides in critical infrastructure and PPP research, future research should focus on the remaining gaps, such as coordination between jurisdictions, entities, and governments. These gaps must be identified in order to craft solutions and identify resources needed to operationalize these policies. Since municipalities are likely to initially lead the incident response for most critical infrastructure, identifying these gaps will help cities, states, and the Federal Government adjust budgets and increase readiness.

Test Coordination Between Cities and States

Future iterations of the JV research program should focus on exercising the coordination among cities, states, and the Federal Government. Cities do not have the same level of resources as states, and are less likely to have sufficient organic personnel and authorities to effectively respond to a cyberspace attack on their own. While states do not have as many resources as the Federal Government, the state level is the first level that can request military assistance in responding to an event.

The most cost-effective outcome of the JV program was the identification, in advance, of critical C2 nodes and personnel who would respond to a cyber-physical incident or attack. By rehearsing the scenario in advance of a natural disaster or man-made event, POCs can be identified in advance. This reduces the time needed to develop an effective and unified response plan during a crisis.

The National Cyber Strategy focuses on the Federal Government, private industry, and international cyber relations, while making no mention of the role of states and local governments in critical infrastructure protection, or even cybersecurity in general.[56]

In addition, if city-state coordination is needed, we must identify the proper procedures for requesting support for different categories of resources. Rather than waiting for an emergency declaration, it may be beneficial for cities and states to request assistance at the first signs of a cyber incident. Physical incident response procedures have been well vetted due to the increased emphasis since 2001. Cybersecurity incident response, which is still not well defined, requires multiple exercise iterations at the state and local level for the development and rehearsing of C2 during these types of incidents.

Develop Coordination Studies

Further studies are needed regarding coordination among industries and coordination between industries and governments. Multiple-sector cybersecurity exercises are still a rarity and fleshing out the dependencies between adjacent sectors is crucial. For example, it would be valuable to see how a power failure would affect healthcare, transportation, and first responders. Likewise, identifying the sectors most dependent on grid power could help companies and governments improve their resilience. Similarly, identifying sectors critical to the government's ability to respond to man-made or natural disasters could ultimately reduce the potential impacts of a cyberspace attack.

[56] Office of the President of the United States, op. cit.

During the JV event, a participant noticed that malicious traffic appeared to be directed at his company from another participant's servers. When the attacked participant was asked how he or she would respond, the participant stated that he or she would probably call his or her buddy in the attacking participant's organization. Currently, there is a reliance on personal relationships, which could be both a help and a hindrance in the event of an attack. If there are personal relationships between members of organizations, information sharing is likely to happen more quickly.

Formalized reporting and sharing procedures between industries and government increase familiarity between industry and government actors and could speed up the identification of anomalous behavior, hasten the notification process, and increase the likelihood of a quicker reaction following an event. While there are considerations about reputation and the ability of an adversary to further exploit a vulnerability if information about it is released publicly, reporting cyber incidents within an industry or industries can reduce the scope of an attack.

Increasing the transparency of incident response, business continuity, and disaster recovery plans may improve best practices within industries and assist governments in identifying critical shortcomings and challenges.

Study Coordinated Attacks on Multiple Cities and States

Future iterations should explore the possibility of a coordinated cyberspace attack spanning multiple cities and states. While such an attack, as far as we know, has not happened, there are no technical barriers to an adversary launching a coordinated attack. This scenario presents a difficult challenge for policymakers due to the separation of geographic jurisdictions.

During a widespread outage or incident response, one must designate a lead agency. Depending on the size and scope of the situation, this may be a federal, state, or local agency. If the attacker is a nation-state, the response may become a Title 10 or DoD action. Most cybersecurity incidents begin with a local law enforcement response. However, defining the thresholds for escalation to the state and federal level and exploring in-depth all possible courses of action are certainly academic research topics worthy of examination. Exploring how to coordinate and communicate across jurisdictions would improve reaction speed and efficacy. Identifying how best to allocate resources among competing emergencies would improve resource prioritization practices and help validate the feasibility of emergency response plans.

Future Scenario Development

In developing future scenarios, ensure that physical events in the scenario do not obscure the need or ability to respond to cyber events. In the JV 2.0 scenario, which combined a hurricane with a cyberspace attack, the hurricane minimized the effects of the cyber events for some industries. While this allowed those industries to keep their damage to a minimum, it prevented them from fully testing their IRPs in a meaningful way.

The preexistent bias of most operators and practitioners is to assume that a system failure is caused by the physical domain. A career-long basis of training in the physical domain is difficult to overcome with a few exercises and a training course. However, we must continue to strive for a balanced approach to incident response and failure resolution in our industrial control systems (ICSs). During future cybersecurity incidents, operational personnel's biases may be used against them to mask the true nature of an attack and convince them that nothing is wrong. Even worse, operational personnel may believe there is something wrong when there is not, thereby inducing a problem themselves. This precarious position is where we find ourselves until we can be sure that we have eliminated and protected ourselves against any possible "ghost in the machine."

4.2. Incorporating, Testing, and Sharing Cyber Education

To improve on the success of the JV project, a cybersecurity education program should be developed. This program should incorporate cybersecurity lessons learned and be tested for its impact on performance, shared with the wider community, and integrated into the curricula of military educational institutions and institutions of higher learning. As participants may have varying levels of experience, every effort should be made to establish a baseline of knowledge to enable meaningful participation.

Test the Ability to Identify a Cyberspace Attack

A future research project should test participants' ability to identify a cyberspace attack. Based on their experiences with previous incident response exercises and training, the cyber maturity level of the organization and participating personnel should be assessed using the Community Cyber Security Maturity Model.[57] The five maturity levels are Initial, Established, Self-Assessed, Integrated, and Vanguard. Based on the initial level of participants, organizational maturity should be increased to the next level or higher by the end of the exercise. For example, if the average participant from an electrical utility is performing at the Initial level (level 1), then the participant should be met where he or she is and the level of the exercise should be crafted so as to guide the organization to the Established or Self-Assessed maturity level (level 2-3). If the participant's entry level is 3, then the participant should be pushed to advance his or her security practices to at least the Integrated level (level 4).[58] Through an iterative process of refining both the participants' plans and the exercise itself, participants should ultimately strive to reach the Vanguard level.

During JV, participants were supplied with the information that they were being attacked so that the exercise could be completed within the given time constraints. However, many of the injects may have taken far longer than a few minutes to identify, and possibly even longer to address.

Add an Educational Component

An educational component of the JV project should be added to inform cities, localities, and states of the value of critical infrastructure protection and their roles in it. The cybersecurity of industry partners should be assessed. In addition, the government workforce should be educated in cybersecurity. We can educate, train, and evangelize corporate America, but if we leave government officials behind, they will remain uneducated and uninspired to develop proactive policies and solutions to problems before they become local, regional, or national crises.

A series of workshops that focused on critical infrastructure protection would not only inform government leaders about the challenges they may face, but also bring diverse private industry representatives and state and local governments together. Establishing partnerships in advance would quicken the notification and cooperation process in the event of an attack.

Integrate Knowledge into Institutional Curricula

Knowledge gained through JV research should be institutionalized through curriculum integration at military educational institutions, such as the U.S. Military Academy and the U.S. Army War College, and at institutions of higher learning, such as the University of Houston and UTSA. Such institutions are well positioned to integrate the operational findings of JV directly into graduate and undergraduate cybersecurity curriculum to educate the future workforce in the critical infrastructure industry and expose it to the current best practices. In this way, the body of knowledge about cybersecurity integration and critical infrastructure protection can be expanded throughout government and private industry and fed back into operator training. This two-way exchange would allow academia to learn from private industry (as it does now in fields such as healthcare and aviation) and, in turn, produce the next generation of leaders for that industry. The use of ISACs and ISAOs should also be considered.

---

[57] Gregory White, "The Community Cyber Security Maturity Model," Proceedings of the 40th Annual Hawaii International Conference on System Sciences, January 3-6, 2007, available from *https://www.researchgate.net/publication/221182620_The_Community_Cyber_Security_Maturity_Model/download.*

[58] Center for Infrastructure Assurance and Security, "The Community Cyber Security Maturity Model," The University of Texas at San Antonio, 2017, available from *http://cias.utsa.edu/the-ccsmm.html.*

4.3. Increase Interactions among IT Personnel, Management, and Senior Leadership

To increase our understanding of incident identification, communication, and response, as well as strategic cyber decision-making, integration must be strengthened between IT and OT personnel and management, and senior leadership should be included as participants in future research.

Involve Senior Leaders as Participants

Senior leaders should actively participate in the exercise, making decisions as to how their organizations will react to the scenario as well as whether to share information with the public or other organizations. While distinguished visitors were able to observe middle management and operators at work, which can give them some insights, it would be beneficial to insert them into the situation so that they can think through strategic actions that they would need to take.

If leaders are not knowledgeable about cyberspace, a baseline understanding would allow them to become actively engaged, making them more able to render decisions as they would need to in a real situation.

One of the most valuable outcomes for many participants in JV was when the senior executive team for each sector met in person the operators who were representing their organizations in the LFX. In many large organizations, there are multiple layers of administration between policymakers and the front-line, day-to-day executors of those policies. Multiple observers during the LFX reported that the most effective exchanges within a single organization were between vertical levels of the team. This vertical integration is critical during a crisis so that decision-makers are aware of the current status minute by minute, and so that they understand the operational impact of their decisions.

Strengthen and Test TTX and LFX Integration

TTX and LFX integration should be strengthened and further tested. The IT professionals of each agency must be integrated into the emergency management planning process and allowed to have operational influence in the exercise. This influence should extend from the exercise to real-life emergencies. It is a common complaint of IT staffs that they are brought into an incident too late, are not consulted for their input, or have no real influence in an incident where technology plays a key role. The decisions that are made in incidents that involve technology will be severely compromised if the IT staff does not play a key role. Because of our world's tremendous reliance on technology in almost all aspects of living, particularly with the advent of the IoT, one can hardly conjure up an incident fact pattern where technology does not play a key role.

This integration must be done formally and under the authority of the principal of the jurisdiction; otherwise, it will be in name only. Any governing or key body that dictates the protocol must include the CIO and the chief information security officer or their top designees. Another added benefit of incorporating the IT staff is the coordination of the cyber incident plans. Though departments within jurisdictions may already have cyber incident plans in place, the departments must ensure that their plans are coordinated, that the procedures in their plans will not thwart the goals of other departments' plans, and that their plans are not at cross purposes with each another.

The ability to respond to a cyberspace attack is also dictated by the resources that a jurisdiction possesses. There should be a centralized process for determining the needed technology procurements for individual agencies so that there is proper continuity of operations and compatibility of resources during an event. IT staff can leverage ISACs to keep the jurisdiction agencies well versed in the current security threats targeting their specific potential, be it personally identifiable information, money, research, or another asset. This networking allows for preparation for targeted attacks and an early warning for the jurisdiction.

4.4. Consistent, Nonattributable Data Collection Is Critical for Future Exercises

Data collection and metrics need further exploration. As a result of the qualitative nature of the research, observers and evaluators should collect the majority of the data throughout the JV series, with a focus on collecting consistent, nonattributable data to inform a replicable framework for future critical infrastructure research. Due to the collaborative nature of the JV project, during the planning conferences, stakeholders must develop specific, measurable, relevant, attainable, and time-based goals for observation during the exercise. Additionally, exploration of an increased role for quantitative data collection may provide further insights.

Standardize Data Collection

Data collection needs to be standardized and consistent. Based on the detailed research goals and metrics stakeholders generate during the planning conferences, a data collection plan must be developed that determines the research questions being answered as well as the methodology for measurement. During JV, several observers took notes, but the notes varied in focus based on the background of the participants. Key stakeholders must develop specific, measurable, attainable, relevant, and time-based goals for observation purposes during the exercise.

Qualitative measurements are designed to test human perception and reasoning. One such methodology is a survey, which can measure the educational background and experience of participants and the rationale behind their actions. Qualitative measurements are designed to gather information from a large group of people quickly. Another type of qualitative measurement is interviews, which take longer, but are likely to provide deeper insights.

Quantitative measurements are designed to test actions taken and the time it took to complete the actions. Cyber range data can provide a wealth of quantitative data, including time taken to discover an anomaly, how the operator reacted to the anomaly, time taken to remediate the anomaly, and how the participant did so.

Balance Operational and Academic Data Collection

In designing data collection procedures, there should be a balance between operational and academic collection, which would require specific guidance as to the attribution of information. This may take place during the collection or sanitization of the information prior to publishing reports. Surveys can be anonymized from the outset by not requiring the name of a participating individual or company to prevent attribution. This also increases the likelihood that the participant will provide honest answers, since they cannot be traced back to the specific individual. The information can still be useful on an operational level if the participant's industry is identified. Quantitative data and observer notes could be traceable to individuals and companies but should be sanitized prior to the release of any reports.

Incorporate JV Findings into a Repeatable Framework

Findings from each iteration of JV should be incorporated into a repeatable framework and used to shape it. Each iteration of JV should build upon the prior versions as well as add new elements to ensure that it does not just become an exercise in testing the current environment. The repeatable framework can then be used by other cities and states to conduct their own exercises, enabling JV to expand at a greater rate.

4.5. Dedicated Research to Understand the Workforce Skill Set

JV has highlighted the need for dedicated research to better understand today's workforce skill sets, determine how they need to evolve, and identify gaps among them. For example, the energy, water, chemical, and defense industrial base sectors rely on ICSs that are becoming more connected to the Internet. As these systems continue to modernize, they will increasingly blend with the electromagnetic spectrum and introduce new vulnerabilities. Training a workforce in these blended environments will continue to be a challenge for the United States. Training must become more available and affordable. With the advent of the IoT, the required skill sets (i.e., the blending of cybersecurity in IT/OT and radio frequency) related to these technologies have yet to be identified. Though the skills necessary for securing infrastructure may increasingly overlap within the workforce, as malicious actors become increasingly adept at remotely interacting with sensitive systems, the differences among skill sets will become more crucial.

Establish Educational Program/Job Duty Fit

Future research should attempt to establish a fit between educational programs for and job duties of participants. The cybersecurity landscape is constantly changing, so ensuring training and educational programs are in line with industry needs is key to ensuring that a workforce is better prepared without requiring extensive on-the-job training. As technology's reach expands and more devices become automated, educational institutions may need to adapt their educational programs to incorporate those changes.

APPENDIX A: ACRONYMS

ACI	U.S. Army Cyber Institute
ARCYBER	U.S. Army Cyber Command
C2	Command and control
CCII	Cybersecurity Control Implementation Interface
CIKR	Critical infrastructure and key resources
CIO	Chief information officer
Citi	Citigroup
Citi-GCTET	Citigroup Global Cyber Threat Exercise Team
CMAW	Cyber Mutual Assistance Workshop
DCIP	Defense Critical Infrastructure Program
DCOE	Defensive Cyberspace Operations Element
DHS	Department of Homeland Security
DIR	Directorate of Information Resources
DoD	Department of Defense
DOE	Department of Energy
DPS	Department of Public Safety
DSCA	Defense Support of Civil Authorities
DSCIR	Defense Support to Cyber Incident Response
EMAC	Emergency Management Assistance Compact
ENISA	European Union Agency for Network and Information Security
EU	European Union
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSARC	Financial Systemic Analysis & Resilience Center
G7	Group of Seven
ICS	Industrial control system
IOC	Indicator of compromise
IoT	Internet of things
IRA	Immediate Response Authority
IRP	Incident response plan
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISP	Internet service provider
IT	Information technology
ITIL	Information Technology Infrastructure Library
JV	Jack Voltaic
LFA	Lead federal agency
LFX	Live-fire exercise
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NICP	NATO Industry Cyber Partnership
NIST	National Institute of Standards and Technology
NYC	New York City
OSD	Office of the Secretary of Defense
OT	Operational technology
PCA	Posse Comitatus Act
POC	Point of contact
PPP	Public-private partnership
R&D	Research and development
SAD	State Active Duty
SCADA	Supervisory Control and Data Acquisition
SDDC	U.S. Army Surface Deployment and Distribution Command
TREAS	Department of the Treasury
TTX	Tabletop exercise
USCYBERCOM	U.S. Cyber Command
UTSA	University of Texas at San Antonio

APPENDIX B: REFERENCES

URLs are valid as of the publication date of this document.

[1] Jonathon Monken, Fernando Maymi, Dan Bennett, Dan Huynh, Blake Rhoades, Matt Hutchison, Judy Esquibel, Bill Lawrence, and Katie Stewart, *Cyber Mutual Assistance Workshop Report*, Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute, 2018, available from *https://resources.sei.cmu.edu/asset_files/SpecialReport/2018_003_001_513596.pdf.*

[2] Army Cyber Institute, *The Cyber Defense Review*, available from *https://cyberdefensereview.army.mil/The-Journal/Publications/*.

[3] Army Cyber Institute, "CyCON U.S.," available from *https://cyber.army.mil/Events/CyCON-US/*.

[4] *Cyber Mutual Assistance Workshop Report*, op. cit.

[5] "National Council of ISACs," National Council of ISACs Website, n.d., available from *https://www.nationalisacs.org/*.

[6] Department of Homeland Security, "Information Sharing and Analysis Organizations (ISAOs)," available from *https://www.dhs.gov/isao.*

[7] Francesca Spidalieri, "State of the States on Cybersecurity," Pell Center for International Relations and Public Policy, Salve Regina University, November 2015, available from *https://pellcenter.org/wp-content/uploads/2017/02/State-of-the-States-Report.pdf.*

[8] ICMA, "Cybersecurity 2016 Survey – Summary Report of Survey Results," April 2017, available from *https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf.*

[9] National Governors Association, "Meet the Threat: States Confront the Cyber Challenge – Memo on State Cybersecurity Strategies," 2016, available from *https://ci.nga.org/files/live/sites/ci/files/1617/docs/1703CybersecurityStrategies.pdf.*

[10] National Defense Authorization Act of 2018, Pub. Law No. 115-91, § 1649 (2018).

[11] *Executive Order 13691*, "*Promoting Private Sector Cybersecurity Information Sharing*," Washington, DC: The White House, February 13, 2015, available from *https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.*

[12] Aaron Mehta, "Pentagon Weighs New Requirements to Secure Military's Vulnerable Power Grid," *Defense News*, November 29, 2017, available from *https://www.defensenews.com/pentagon/2017/11/29/pentagon-weighs-new-requirements-to-secure-militarys-vulnerable-power-grid/*.

[13] Department of the Army, "Moving the Army Texas Style," *Army Logistician*, July-August 2004, available from *https://alu.army.mil/alog/issues/julaug04/texas.html.*

[14] Department of Homeland Security, "Critical Infrastructure Partnership Advisory Council," updated March 29, 2019, available from *https://www.dhs.gov/critical-infrastructure-partnership-advisory-council.*

[15] Joey Cheng, "DOD Switches to NIST Security Standards," *Defense Systems*, April 3, 2014, available from *https://defensesystems.com/articles/2014/04/03/dod-adopts-nist-security-standards.aspx.*

APPENDIX B: REFERENCES (CONT.)

URLs are valid as of the publication date of this document.

[16] Scott Maucione, "TRANSCOM Worried About Cybersecurity Gap Between DoD and Civilian Networks," *Federal News Network*, March 30, 2017, available from *https://federalnewsnetwork.com/cybersecurity/2017/03/transcom-worried-cybersecurity-gap-dod-civilian-networks/.*

[17] National Institute of Standards and Technology, "DFARS Cybersecurity Requirements," U.S. Department of Commerce, updated June 28, 2018, available from *https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance.*

[18] National Institute of Standards and Technology, "Cyber Risk Management," U.S. Department of Commerce, updated October 17, 2018, available from *https://www.nist.gov/mep/cybersecurity-resources-manufacturers/cyber-risk-management.*

[19] City of Houston, "Cybersecurity Control Implementation Interface," available from *https://www.cciitool.info/splash.*

[20] Office of the President of the United States, "National Cyber Strategy of the United States of America," Washington, DC: The White House, September 2018, available from *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.*

[21] U.S. Department of Defense, "Summary: Department of Defense Cyber Strategy," Washington, DC: U.S. Department of Defense, 2018, available from *https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.*

[22] NATO Communications and Information Agency, "NATO Industry Cyber Partnership (NICP)," North Atlantic Treaty Organization, available from *https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx.*

[23] Ibid.

[24] "NATO Cooperative Cyber Defense Centre of Excellence," NATO Cooperative Cyber Defense Centre of Excellence Website, n.d., available from *https://ccdcoe.org/.*

[25] General Secretariat of the Council, "EU to Create a Common Cybersecurity Certification Framework and Beef Up its Agency – Council Agrees its Position," Council of the European Union, June 8, 2018, available from *https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/.*

[26] European Union Agency for Network and Information Security, "National Cyber Security Strategies," European Union, available from *https://www.enisa.europa.eu/topics/national-cyber-security-strategies.*

[27] Group of Seven, "G7 Principles and Actions on Cyber," U.S. Department of State Website, March 13, 2016, available from *https://2009-2017.state.gov/s/cyberissues/releasesandremarks/258028.htm.*

[28] Posse Comitatus Act of 1878, 18 U.S.C. § 1385 (1878).

[29] Stafford Disaster Relief and Emergency Assistance Act of 1988, Pub. Law No. 100-707 (1988).

[30] Economy Act of 1933, 38 U.S.C. § 701 (1933).

[31] Major General Tim Lowenberg National Guard Cyber Defenders Act of 2018, S. 2887, 115th Congress (2018).

[32] Isaac R. Porsche III, Caolionn O'Connell, John S. Davis II, Bradley Wilson, Chad C. Serena, Tracy C. McCausland, Erin-Elizabeth Johnson, Brian D. Wisniewski, and Michael Vasseur, *Cyber Power Potential of the Army's Reserve Component*, Santa Monica, CA: RAND Corporation, 2017, available from *https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1490/RAND_RR1490.pdf.*

[33] National Guard Bureau, "NG Cyber Defense Team," United States National Guard, updated December 2017, available from *https://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/NG%20Cyber%20Defense%20Team%20Fact%20Sheet%20(Dec.%202017).pdf.*

[34] Ibid.

[35] Federal Emergency Management Agency Emergency Management Institute, "IS-75: Military Resources in Emergency Management," presentation, n.d., available from *https://training.fema.gov/emiweb/is/is75/visuals/visuals%20-%20powerpoint.pptx.*

[36] State of Connecticut, "Cybersecurity Action Plan," May 2, 2018, available from *https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en.*

[37] Kate Brumback, "Cyberattacks Wakeup Call for Local Governments to Prepare," *Associated Press*, March 30, 2018, available from *https://www.apnews.com/1c599d36222544e1928e07b62bd9b713.*

[38] Stephen Deere, "Confidential Report: Atlanta's Cyber Attack Could Cost Taxpayers $17 million," *The Atlanta Journal-Constitution*, August 1, 2018, available from *https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWIMcXS0K/?icmp=np_inform_variation-control.*

[39] State of Connecticut, op. cit.

[40] Chris Bing, "Inside 'Project Indigo,' the Quiet Info-Sharing Program between Banks and U.S. Cyber Command," *CyberScoop*, May 21, 2018, available from *https://www.cyberscoop.com/project-indigo-fs-isac-cyber-command-information-sharing-dhs/*.

[41] Paul Chichonski, Tom Millar, Tim Grance, and Karen Scarfone, *NIST Special Publication 800-61: Computer Security Incident Handling Guide*, *Revision 2*, Gaithersburg, MD: U.S. Department of Commerce, August 2012, available from *https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.*

[42] City of Houston, op. cit.

[43] United States Computer Emergency Readiness Team, "Critical Infrastructure Cyber Community Voluntary Program," U.S. Department of Homeland Security, available from *https://www.us-cert.gov/ccubedvp.*

[44] San Diego Cyber Center of Excellence, *San Diego Region-Wide Cyber Incident Response Guide*, City of San Diego, October 2017, available from *https://sdccoe.org/wp-content/uploads/2017/10/San-Diego-Cyber-Incident-Response-Guide-10-17.pdf.*

[45] California Cyber Security Integration Center, *California Joint Cyber Incident Response Guide,* California Office of Emergency Services, February 27, 2018, available from *https://www.caloes.ca.gov/LawEnforcementSite/Documents/California-Joint%20Cyber%20Incident%20Response%20Guide.pdf.*

APPENDIX B: REFERENCES (CONT.)

URLs are valid as of the publication date of this document.

[46] *DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)*," Washington, DC: U.S. Department of Defense, December 29, 2010, available from *https://www.dco.uscg.mil/Portals/9/CG-5R/nsarc/DoDD%20 3025.18%20Defense%20Support%20of%20Civil%20Authorities.pdf.*

[47] Jim Finkle and Christopher Bing, "U.S. Seeks More Cooperation with Private Sector to Fight Cyber Attacks," *Insurance Journal*, August 1, 2018, available from *https://www.insurancejournal.com/news/national/2018/08/01/496636.htm.*

[48] Deputy Secretary of Defense, *Directive-Type Memorandum 17-007: Interim Policy and Guidance for Defense Support to Cyber Incident Response*, Washington, DC: Office of the Secretary of Defense, updated May 25, 2018, available from *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dtm/DTM-17-007. pdf?ver=2018-05-25-080104-323.*

[49] *DoD Directive 3025.18*, op. cit.

[50] *Joint Publication 3-28, "Defense Support of Civil Authorities*," Washington, DC: Joint Chiefs of Staff, U.S. Department of Defense, October 29, 2018, available from *https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf.*

[51] *Presidential Policy Directive 41, "United States Cyber Incident Coordination*," Washington, DC: The White House, July 26, 2016, available from *https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/ presidential-policy-directive-united-states-cyber-incident.*

[52] Antideficiency Act of 1982, 31 U.S.C. § 1341 (1982).

[53] Posse Comitatus Act of 1878, op. cit.

[54] Ibid.

[55] Computer Fraud and Abuse Act of 1984, 18 U.S.C. § 1030 (1984).

[56] Office of the President of the United States, op. cit.

[57] Gregory White, "The Community Cyber Security Maturity Model," Proceedings of the 40th Annual Hawaii International Conference on System Sciences, January 3-6, 2007, available from *https://www.researchgate.net/ publication/221182620_The_Community_Cyber_Security_Maturity_Model/download.*

[58] Center for Infrastructure Assurance and Security, "The Community Cyber Security Maturity Model," The University of Texas at San Antonio, 2017, available from *http://cias.utsa.edu/the-ccsmm.html.*

APPENDIX C: PUBLIC AFFAIRS OFFICE RECOMMENDED LANGUAGE

A public affairs strategy must be in place prior to a cyberspace attack with cascading effects that impact multiple sectors. It is critical to have a shared understanding of the correct messages and products and who the release authority is for an actual, real-world crisis to ensure that responses are succinct and accurate and that organizations are unified in releasing information to the public.

States should develop templates for press releases, products, and broad messaging that can be tailored later to specific events. Examples of these broad messages include the following:

- Every day, the department of _____ is working diligently to respond to requests relating to its core tasks.
- The safety and security of our citizens is our top concern.
- Our responders are working around-the-clock to bring _____ back to our citizens. For more information on how to help or provide our department with updates, please visit our website at _____ or call our hotline at _____.

The ACI Public Affairs Office provided the following language to consider using when developing press releases:

- _____ will be in charge of updating the public during or immediately following the _____ incident with a statement via social media.
- A more detailed press release/statement about the incident should be released within ___ hours of the incident.
- Within ____ hours or days, a press conference will be held where ____ will address the following issues/ concerns about the incident.
- Within _____days or hours of the event, public affairs or public relations officials should hold a synchronization meeting to ensure all parties, members, and organizations understand all details of the incident and how to better assist the lead.

APPENDIX D: JV-DRIVEN DEFENSE BILL PROVISION

JV's strategic impact shows that the highest levels of government recognize the Nation's need to establish preparedness for inevitable national disasters and cyberspace attacks through these exercises. JV provides a forum where stakeholders can meet in a low-threat environment to forge these critical relationships, instead of waiting for a massive attack to occur to do so.

SEC. 1649. PILOT PROGRAM ON MODELING AND SIMULATION IN SUPPORT OF MILITARY HOMELAND DEFENSE OPERATIONS IN CONNECTION WITH CYBER ATTACKS ON CRITICAL INFRASTRUCTURE.

(a) PILOT PROGRAM REQUIRED.—

(1) IN GENERAL.—The Assistant Secretary of Defense for Homeland Defense and Global Security shall carry out a pilot program to model cyber attacks on critical infrastructure in order to identify and develop means of improving Department of Defense responses to requests for DSCA for such attacks.

(2) RESEARCH EXERCISES.—The pilot program shall source data from and include consideration of the ''JV'' research exercises conducted by the Army Cyber Institute, industry partners of the Institute, and the cities of New York, New York, and Houston, Texas.

(b) PURPOSE.—The purpose of the pilot program shall be to accomplish the following:

(1) The development and demonstration of risk analysis methodologies, and the application of commercial simulation and modeling capabilities, based on artificial intelligence and hyperscale cloud computing technologies, as applicable—

(A) to assess defense critical infrastructure vulnerabilities and interdependencies to improve military resiliency;

(B) to determine the likely effectiveness of attacks described in subsection (a)(1), and countermeasures, tactics, and tools supporting responsive military homeland defense operations;

(C) to train personnel in incident response;

(D) to conduct exercises and test scenarios;

(E) to foster collaboration and learning between and among departments and agencies of the Federal Government, State and local governments, and private entities responsible for critical infrastructure; and

(F) improve intra-agency and inter-agency coordination for consideration and approval of requests for defense support to civil authorities.

(2) The development and demonstration of the foundations for establishing and maintaining a program of record for a shared high-fidelity, interactive, affordable, cloud-based modeling and simulation of critical infrastructure systems and incident response capabilities that can simulate complex cyber and physical attacks and disruptions on individual and multiple sectors on national, regional, State, and local scales.

(c) REPORT.—

(1) IN GENERAL.—At the same time the budget of the President for fiscal year 2021 is submitted to Congress pursuant to section 1105(a) of title 31, United States Code, the Assistant Secretary shall, in consultation with the Secretary of Homeland Security, submit to the congressional defense committees a report on the pilot program.

(2) CONTENTS.—The report required by paragraph (1) shall include the following:

(A) A description of the results of the pilot program as of the date of the report.

(B) A description of the risk analysis methodologies and modeling and simulation capabilities developed and demonstrated pursuant to the pilot program, and an assessment of the potential for future growth of commercial technology in support of the homeland defense mission of the Department of Defense.

(C) Such recommendations as the Secretary considers appropriate regarding the establishment of a program of record for the Department on further development and sustainment of risk analysis methodologies and advanced, large-scale modeling and simulation on critical infrastructure and cyber warfare.

(D) Lessons learned from the use of novel risk analysis methodologies and large-scale modeling and simulation carried out under the pilot program regarding vulnerabilities, required capabilities, and reconfigured force structure, coordination practices, and policy.

(E) Planned steps for implementing the lessons described in subparagraph (D).

(F) Any other matters the Secretary determines appropriate.

ARMY CYBER
INSTITUTE
AT WEST POINT