Jack Voltaic®: Bolstering Critical Infrastructure Resilience

Major General Robin L. Fontes
Major Erik Korn
Lieutenant Colonel Doug Fletcher
Major Jason Hillman
Lieutenant Colonel Erica Mitchell
Major Steven Whitham

ABSTRACT

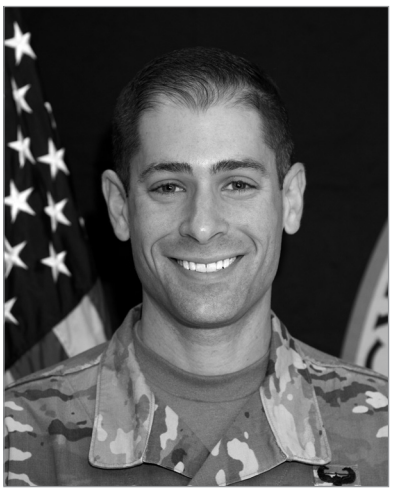
According to the Department of Homeland Security (DHS), municipal critical infrastructure has become an ideal target for a range of cyber threat actors including near-peer competitors seeking geopolitical gains and decentralized cyber criminals attempting to hold cities captive for monetary gain.[1] With municipalities predominantly partnering with the private sector for operation of national critical infrastructure as defined in Presidential Policy Directive (PPD) 21, cities, states, and industry entities find themselves on the front lines—possibly the first line of defense—against a perpetual barrage of attacks in cyberspace.[2] Accordingly, a dynamic shift from traditional conflict in the physical world to a homeland defense posture in cyberspace reveals several potential gaps with regard to handling emergency situations, coordinating response efforts, and restoring basic services for citizens.[3] This article seeks to highlight this dynamic environment, and the inherent gaps that exist in bolstering critical infrastructure resilience. Accordingly, the Jack Voltaic® (JV) research framework discussed in this article explores the interconnections among municipal, state, and federal response efforts during a cyber emergency scenario, with added emphasis on critical findings and themes from its Jack Voltaic® 2.5 workshop series. This effort brought together key regional stakeholders from across various levels of governance, the private sector, and academia to discuss the findings of previous JV exercises, lessons learned, and how similar efforts can strengthen critical infrastructure, community resilience, and a whole-of-nation approach to handling cyber threats.[4] This article will highlight common findings and themes from multiple exercises and workshops that further reinforce current JV research and the Jack Voltaic® 3.0 Legal and Policy Tabletop Exercise (TTX). Finally, this article concludes with a detailed discussion about JV 3.0, which is scheduled to execute in September 2020.

Keywords *– Jack Voltaic®, Resilience, Critical Infrastructure, Defense Support of Civil Authorities, Defense Support to Cyber Incident Response, Defender 2020, Multi-Domain Operations.*

Major General Robin L. Fontes has served as Deputy Commanding General (Operations), U.S. Army Cyber Command, since December 2019. She graduated from the U.S. Military Academy at West Point, N.Y., in May 1986 and commissioned as a second lieutenant in the Military Police Corps. During her career, she has served in a number of command, staff, and joint positions. She has commanded at all levels from a company to the Combined Security Transition Command-Afghanistan. Maj. Gen. Fontes has completed five operational assignments in Afghanistan, including four tours supporting OPERATION ENDURING FREEDOM and one tour in support of OPERATION FREEDOM'S SENTINEL. She has earned a Bachelor's degree from the U.S. Military Academy, Master's degrees in International Affairs from the University of Washington and National Security and Strategic Studies from the National Defense University.

SCENE SETTER

An international crisis in Europe prompts the U.S. President to order the rapid deployment of two brigade combat teams as a show of force in support of US allies. Tensions remain high at home and abroad as similar threats arise on both fronts. Forces are needed immediately, and any delay further harms US and NATO interests. US and NATO adversaries begin an immediate cyber assault on domestic critical civilian-owned infrastructure at first, but attacks quickly spread to critical NATO port cities as well. Gas pipelines rupture and transmission nodes are disrupted, causing interruption in fuel distribution.[5] *Widespread power outages lead to mass disruption of public utilities,*[6] *overloading of municipal medical systems, and civil unrest. Social media and news outlets report on these catastrophes, exacerbating negative public sentiment. Traffic systems become overloaded,*[7] *bringing vehicles to a standstill across strategic port cities and thus delaying access to the ports. Emergency operations centers at the municipal and state levels are unable to deal with this myriad of crises. Governors activate their state National Guard units in response to emergency declarations. Agency directors and Defense Coordination Officers become overrun with support requests from every region. Meanwhile, cargo manifests for rail and load plans at the ports are manipulated, causing incorrect heavy equipment loads. Some ships partially overturn in port*[8], [9]*; commercial and military shipping is blocked along the east coast.*[10] *Military equipment is delivered to the wrong destination and becomes significantly delayed. Garrison Commanders lose visibility of their personnel and equipment and cannot reach local authorities for resolution. Combatant Commanders around the world are faced with the responsibility of responding to adversaries, not knowing where their equipment is or when it will arrive. The Federal Bureau of Investigation and Department of Homeland Security commit teams to investigate and mitigate these local disasters. However, by the time it is understood that this is a coordinated cyberattack and force projection operations resume, the US has failed to respond in a timely manner, resulting in strategic disaster.*



Major Erik Korn is a U.S Army Cyber Officer serving as a Research Scientist at the Army Cyber Institute (ACI) at the United States Military Academy (USMA). Erik attained a B.S. in Comparative Politics from USMA in 2009, and an M.P.A. from Columbia University School of International and Public Affairs (SIPA) in 2018. MAJ Korn has previously served in a variety of operational Military Intelligence (MI) and Cyber assignments, including Brigade Collection Manager, ISR Platoon Leader, MI Company Executive Officer, Cyber Mission Commander, and Cyber Company Commander. He currently serves as a member of the ACI's Critical Infrastructure Key Resources (CIKR) Research Team, as well as the Jack Voltaic® 3.0 Data Collection and Analysis Lead. Erik also serves as a co-Course Director for the USMA Department of Electrical Engineering and Computer Science (EECS) IT460 Cyber Policy, Strategy, and Operations course, and faculty advisor for the cadet Cyber Policy Team.

INTRODUCTION

As outlined in the U.S. Cyber Command (USCYBERCOM) Command Vision, the globally interconnected digital nature of cyberspace and continuing proliferation of technology makes critical infrastructure a prime target for a multitude of persistent cyber threats.[11] With over 85% of US critical infrastructure owned and operated by the private sector, threats to the homeland are no longer across oceans or borders; they persistently reside within the domestic critical systems that American citizens depend on for basic services, safety, and security.[12] Cyberattacks in the form of denial of service, ransomware, and phishing are just some of the methods that can deliver debilitating effects against vulnerable critical domestic systems.[13] Increasingly sophisticated attack techniques and porous defenses within the US together make plausible a scenario in which a private company stands as the first line of defense against an attacking nation state. According to a recent December 2019 report, cyberattacks against local governments are reaching "critical" mass, citing as many as 948 municipalities, school systems, and health care providers reporting impacts by just ransomware alone.[14] Moreover, early decisions made by affected entities may set precedent for national response, and even in some ways constrain it. Recognizing the urgency of this growing threat, the Army Cyber Institute (ACI) at West Point launched the Jack Voltaic® (JV) research series aimed at studying critical infrastructure vulnerabilities in collaboration with industry and local government stakeholders to improve resiliency in interdependent systems from the bottom-up.

BACKGROUND

JV is the ACI's research project that focuses on the study of critical infrastructure resiliency and public-private partnerships, as well as municipal cyber incident response, recovery, and remediation efforts. In addition to supporting increased critical infrastructure

Lieutenant Colonel Doug Fletcher is a U.S. Army Operations Research Systems Analyst Officer currently serving as a Senior Research Scientist at the Army Cyber Institute at the United States Military Academy. Doug attained a B.S. in Applied Mathematics from the United States Military Academy in 1997, an M.S. in Applied Mathematics from the Naval Postgraduate School in 2007, and his Ph.D. in Statistics from Temple University in 2019. He is currently the project lead for Jack Voltaic® 3.0, a research event into how cyberattacks against commercial critical infrastructure impact Army force projection. Doug's current research interests include exercise design, statistical learning, and generalized linear modeling.

resiliency, this initiative also works to better inform our understanding of the nation's dependence on local governance and civilian critical infrastructure, specifically potential impacts on force projection capabilities in the event of local disruption. The JV concept grew from the energy sector's efforts in developing cyber mutual assistance, supporting sector coordination and resourced responses to major cyber incidents.[15] JV expands this concept across multiple sectors of critical infrastructure as a result of the interconnected nature of cyberspace, creating both sector-specific and multi-sector dependencies. Whereas most federal efforts aim at improving resiliency focus on regional or multi-state emergency response, JV takes a unique approach by focusing on the city level, where the density of both critical infrastructure and population is greatest. This bottom-up approach identifies key stakeholders and public-private partnerships, experimental design elements, governance hierarchies, exercise simulations, and relevant data collection points to elucidate critical insights regarding existing gaps, vulnerabilities, and successes of cyber incident response.[16] These unique bottom-up perspectives thus personify the critical need for integrating security considerations into incident response at all levels, and thereby helps to codify real-world cyber emergency response efforts to alleviate confusion during the heat of a real crisis.

The ACI began this effort in 2016 with Jack Voltaic® 1.0. In partnership with Citigroup, this event brought together private sector, federal, state, and local government stakeholders to simulate a "Cyber Worst Day" scenario in which key segments of New York City's critical infrastructure became severely degraded as a result of a cyber incident. This iteration of JV featured both adversary and friendly response network engagements in a simulated environment in parallel with a key leader tabletop exercise (TTX). The two-day event in New York City involved 25 organizations and 137 participants from 6 different critical infrastructure sectors: Financial Services, Emergency Services, Communications,

Major Jason Hillman is a Cyber Strategist and Research Scientist for the Army Cyber Institute at West Point. He also serves as an instructor in the U.S. Military Academy's Electrical Engineering and Computer Science Department. Jason graduated from West Point with a B.S. in Systems Engineering in 2005 and earned an M.S. in Cybersecurity from Webster University in 2018. His military service includes serving at increasing levels of responsibility starting at the tactical level as a platoon leader, up to and including Deputy Chief of Operations for Combined Security Transition Command - Afghanistan. Jason's primary research focus at ACI is critical infrastructure resilience. He maintains the following military skills and industry certification: Strategic Planner (6Z), Joint Planner (3H), Joint Cyber Operations Planner (3K), Space Enabler (3Y), Certified Information System Security Professional (CISSP).

Healthcare, Energy, and Transportation Systems.[17] In addition to establishing critical partnerships among the ACI, New York State, and New York City (NYC), it also helped NYC create a new cybersecurity agency, the New York City Cyber Command (NYC3).[18] The key findings from the first iteration emphasized the importance of a rehearsed city-level response plan nested within the state and federal response. While there are existing means at the federal and state level to enable cyber preparation, prevention, and response, it remains imperative that cities also develop, practice, and support their own cyber incident response.

The second iteration of JV took place with the city of Houston in partnership with infrastructure company Architecture Engineering Construction Operations and Management (AECOM) and Cybersecurity firm Circadence, again focusing closely on the study of potential gaps in resilience, emergency municipal coordination, and appropriate incident response. Jack Voltaic® 2.0 sought to expand on the previous iteration through exploration of a cyberattack following the occurrence of a devastating hurricane. Furthermore, by including elements in the scenario that affected the port of Beaumont, TX, this iteration of JV explored impacts on the Army's ability to deploy forces in defense of the nation due to a physical incident and cyberattack on a large American port city. JV 2.0 consequently assisted in establishing critical partnerships between government and industry, thereby enabling new Army public-private partnerships to take shape. JV 2.0 provided numerous findings and lessons learned, resulting in its inclusion in the 2019 National Defense Authorization Act Section 1649 as a method to assess and analyze critical infrastructure resiliency.[19] Two key findings of JV 2.0 furthered multi-level government cyber incident response. First, policy and legal authorities at the federal and state levels should be reviewed and adjusted to enable and complement cyber incident response at the city level.[20] Furthermore, current physical and cyber incident response frameworks require a review from

Lieutenant Colonel Erica Mitchell is the Critical Infrastructure and Key Resources (CIKR) Research Group Chief for the Army Cyber Institute and Assistant Professor in the Electrical Engineering and Computer Science Department at the United States Military Academy (USMA) at West Point. She graduated from West Point with a B.S. in American Legal Systems, was commissioned as a Signal Corps officer, and later transitioned to an Information Systems Management Officer (FA26B). She earned an M.S. in Information Systems Management, C.A.S. in Information Security Management, and Ph.D. in Information Science and Technology from Syracuse University. Her military service includes serving at increasing levels of responsibility, starting at the tactical level as a platoon leader, up to and including project management on DoD-level enterprise technology programs. Her main research focus at ACI is critical infrastructure resilience. She is a member of ACM and ISC2 and maintains the CISSP certification.

city to state to federal ("bottom-up") to allow the most flexibility in response to the rapidly evolving threat of cyberattacks.[21] In addition to these critical insights on cyber incident response, the second iteration of JV further illuminated the importance of civil and commercial critical infrastructure for the U.S. Army and helped guide additional research focus areas for Jack Voltaic® 3.0.[22]

While exercises in JV 1.0 and 2.0 produced findings and insights that support improved critical infrastructure resiliency, there are also other complementary events that contribute to achieving the overarching series objectives. These events highlight unique stakeholder insights on authorities, mitigation, and remediation that together identified a need for building municipal incident response frameworks capable of simultaneously addressing both cyber and physical incidents; this includes "cross-border and city-state-National Guard cooperation" that can further facilitate cyber personnel and capability resource sharing across existing structures.[23] In addition to planning workshops that support a specific exercise, a series of smaller one-day city-focused JV 2.5 workshops provided individual cities an opportunity to learn from the Jack Voltaic® research series, discuss how those findings apply to their environment, and improve partnerships across local sectors.

FINDINGS AND RECOMMENDATIONS

1. Crisis management and remediation is personality driven.

While the original research thesis centered around establishing structural lines of communication to mitigate personnel changeover, comments from participants and observations during Jack Voltaic® events have led to a contrary broader and somewhat different conclusion. Rather than just documenting lines of communication to draw upon during an actual crisis, it became apparent that individuals from disparate

Major Steven Whitham is a cyber warfare officer serving as a research scientist at the Army Cyber Institute. MAJ Whitham graduated with a B.S. in Computer Science from the United States Military Academy at West Point in 2009 and M.S. in Computer Science from the University of Washington in 2018. He is currently the lead scenario designer for the Jack Voltaic® research project. His research areas of interest include machine learning, artificial intelligence, cybersecurity, and exercise design.

organizations primarily rely on those they know. Rather than fight this tendency, organizations can better encourage familiarity among individuals and groups through regularly hosted events to build essential interpersonal and professional bonds for cyber incident response. Encouraging key personnel from distinct organizations, especially those in municipal emergency management, to attend these events is critical to improving communication across sectors and will ultimately lead to enhanced resilience. We recommend municipalities place strong emphasis on developing personal relationships and exchanging contact information during emergency preparedness drills in addition to practicing response actions and organizational responsibilities.

2. Individuals and organizations tend to lack experience with real cyber events and thus have difficulty visualizing second-, third-, and fourth-order effects; this inhibits a true understanding of interdependencies among organizations.

Municipalities, private companies, and other critical stakeholders typically conduct self-contained drills that unintentionally gloss over second-, third-, and fourth-order effects, ultimately detracting from a more complete understanding of the impacts to their organizations and subsequent interdependencies. During JV workshops, participants were able to identify the immediate impacts that cyber events would have on their organizations but generally lacked the ability to extend that impact to other interdependent entities. Full understanding of interdependencies is difficult to imagine in advance, but without exception participants in JV workshop events commented on learning about how much their organizations truly rely on other sectors, and how much other organizations relied on theirs. Participants from local government who participated in the planning for a full Jack Voltaic® scenario also remarked how the act of simply coming together for a planning workshop was a huge boon for them, raising interrelated

issues they had never thought to consider and introducing participants to key personalities, even within the local area. We recommend crisis management drills incorporate as broad a set of interested parties as possible from public and private sectors, at all levels of responsibility. Additionally, we recommend moderators for such drills allow time for participants to exercise creativity in considering how effects and responses to events may cause ripple effects, especially in prioritizing resources during incident response.

3. Municipalities and private entities tend to lack cyber policies, whether specific frameworks or as annexes to existing crisis management policies, and too often treat cyber incidents as information technology concerns.

Accordingly, when cyber incidents lead to physical events, existing crisis management documentation does not specify thresholds beyond the most extreme events and appear insufficient to handle situations wherein the causes of problems (cyber or mechanical) are not immediately known. Emergency management and incident response must therefore start including cyber as one of its critical components. Cyber intrusions are predominately considered an information technology (IT), not operational, problem at numerous levels of governance. Leaders often fail to recognize that the operation and maintenance of IT systems is a discipline and skill set unto itself. IT professionals may share underlying technical knowledge with IT security professionals, but their expertise and focus areas are dramatically different. This gap is further exacerbated with respect to operational technology (OT), the systems which undergird industrial infrastructure. Our JV workshops highlight a shortfall in understanding the full scope of threats to municipal critical infrastructure that currently exist with respect to building both IT and OT resilience. Leaders of organizations must stop treating cyber intrusion as a purely IT problem and begin treating it as an operational problem. Cities also tend to lack adequate cyber response policies in the form of specific documentation or as annexes to existing crisis management policies. This gap highlights the necessity of these critical stakeholders having these important conversations during events like JV in order to identify, discuss, and address previously siloed response actions that do not address important security considerations across sectors, community lifelines, and critical organizations. Additionally, even after including cyber events into existing crisis drills, incorporating effective measures, and resourcing them can take years for full maturation. We recommend organizations and municipalities incorporate scenario events into their regular drills designed to exploit gaps in current policy and force decision points that currently are not clearly defined.

4. Municipalities and organizations generally do not know what resources are available or who provides them during a cyber event; this results in hesitancy to declare a cyber incident.

Cyber incidents are by nature more difficult to identify than physical events, especially when a cyber intrusion causes a physical event. Federal and state resources are available across the country to assist with cyber incidents, but these resources may be slow to arrive if

it takes time to ascertain cyber intrusion as a cause. This can lead to a situation where those municipalities that have the greatest need for support lack the initial resources to determine what factors qualify them to request it. Exacerbated by the reality of our previous finding regarding policies, municipality emergency response personnel are often reluctant to claim a cyber incident is occurring, even at cyber resilience workshops, because their policies do not allow for such a declaration without higher approval. Local government and private sector participants at workshops were often surprised to learn that resources were available from entities like DHS, or that some states have extended their State Emergency Assistance Compacts to include cyber incident response. Federal-level cyber exercises tend to be held at state and regional levels, attempting to provide the greatest support to the biggest area. Unfortunately, this tends to leave municipality personnel unaware of available cyber resources. We recommend municipality drills include scenario events designed to exhaust locally available resources due to effects from cyber incidents, thus forcing participants to make resource requests and establish important lines of communication with supporting entities.

CONCLUSION AND WAY FORWARD WITH JACK VOLTAIC® 3.0 EXECUTION

The next full iteration of this research framework will occur with Jack Voltaic® 3.0, planned for September 2020. In concert with industry, municipal, and academia partners, the ACI will continue to study local response efforts during a multi-sector and multi-location cyber incident. This JV iteration will specifically focus on the cascading impacts of a cyberattack against municipal critical infrastructure, and how this affects the Army's ability to deploy and project forces. The third iteration of this study is currently finalizing plans and will occur as a completely distributed event in September 2020 with both the cities of Charleston, South Carolina, and Savannah, Georgia.

The JV3.0 exercise remains focused on examining and analyzing the impact of a cascading cyber incident delivering a range of effects against municipal critical infrastructure, the same critical infrastructure upon which the nation depends for its force projection capabilities. US port facilities exemplify one such critical infrastructure on which the Army depends on for force projection. A recent cyber incident in December 2019 resulted in 30 hours of degraded operations at a single maritime facility, demonstrating just how much damage can be inflicted with the occurrence of a similar cascading event occurring at multiple port facilities.[24] Accordingly, outlined research objectives for this iteration remain focused on building resiliency from the bottom-up, while also studying consequent impacts on the nation's ability to quickly move soldiers, equipment, and supplies to an active and potentially hostile area of operations (AO). As such, concerted efforts were made to nest earlier JV 3.0 events with the Army's DEFENDER-Europe 2020 exercise, the largest exercise covering deployment from the US to Europe in over 25 years.[25] This exercise will consequently bring together municipal, county, state, and federal stakeholders, along with critical members of industry and academia, to continue building comprehensive and holistic domestic critical

infrastructure resilience. Jack Voltaic® 3.0 will therefore focus on examining the following targeted research objectives:

- Exercise multiple cities in emergency cyber incident response, both for ensuring public services and safeguarding critical infrastructure.
- Reinforce a "whole-of-community" approach in response to cyber events through sustained multi-echelon partnerships across industry, academia, and government.
- Examine the coordination process for providing cyber protection capabilities in support of Defense Support of Civil Authorities (DSCA) requests.
- Develop a repeatable and adaptable framework that allows cities to exercise its response to multi-sector cyber incidents.
- Examine how cyberattacks on civilian critical infrastructure impact force projection.

Through these mutually supporting objectives, JV3.0 remains committed to building domestic critical infrastructure resiliency, facilitating partnerships, addressing gaps, codifying interdependencies, reinforcing holistic and comprehensive solutions to cyber incident response, and better enabling a whole-of-community approach. These factors not only ubiquitously affect force projection capabilities, but also directly impact the safety, security, and resilience of the American people. In a time characterized by Multi-Domain complexities within an emerging operational environment, defense of the homeland remains a paramount function of this effort.[26] The National Security Strategy (NSS) further reinforces this function, specifically highlighting the importance of critical infrastructure resiliency as a crucial facet of national protection, capabilities, and defense efforts; this includes deterring and disrupting malicious cyber threat actors from inflicting "catastrophic or cascading consequences."[27] Accordingly, the Jack Voltaic® Research Series seeks to facilitate comprehensive solutions, reinforce a whole-of-nation approach, and adequately address persistent challenges within this interdependent threat landscape that increasingly includes US homeland municipalities.

NOTES

1. "Secure Cyberspace and Critical Infrastructure," Department of Homeland Security, October 24, 2019, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.
2. "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience" (The White House, February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
3. Erica Mitchell, et al., "Jack Voltaic Critical Infrastructure and Public-Private Partnerships," *ACI Technical Reports*, July 18, 2019, 20-29, https://digitalcommons.usmalibrary.org/aci_rp/42.
4. "Jack Voltaic® 2.5: Cyber Workshop Series" (The Army Cyber Institute, 2019), https://cyber.army.mil/Portals/3/Documents/JackVoltaic/Jack%20Voltaic%202_5%20InfoSheet_v4.pdf?ver=2019-08-20-153840-620.
5. Kate O'Flaherty, "U.S. Government Issues Powerful Cyberattack Warning As Gas Pipeline Forced Into Two Day Shut Down," February 21, 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/02/19/us-government-issues-powerful-cyberattack-warning-as-gas-pipeline-forced-into-two-day-shut-down/.
6. Brian Barrett, "An Unprecedented Cyberattack Hit US Power Utilities," *Wired* (Conde Nast, September 7, 2019), https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/.
7. Eduard Kovacs, "Critical Vulnerability Could Have Allowed Hackers to Disrupt Traffic Lights," *SecurityWeek*, June 5, 2020, https://www.securityweek.com/critical-vulnerability-could-have-allowed-hackers-disrupt-traffic-lights.
8. Ken Munro, "Sinking a Ship and Hiding the Evidence," Pen Test Partners RSS, February 18, 2019, https://www.pentestpartners.com/security-blog/sinking-a-ship-and-hiding-the-evidence/.
9. Tara Seals, "Researcher: Not Hard for a Hacker to Capsize a Ship at Sea," *Threatpost English Global,* threatpost.com, February 20, 2019, https://threatpost.com/hacker-capsize-ship-sea/142077/.
10. Alex Johnson, "After 'Pure Horror' of Rescue, Authorities Ponder What to Do with the Golden Ray," NBCNews.com (NBCUniversal News Group, September 11, 2019), https://www.nbcnews.com/news/us-news/after-pure-horror-rescue-authorities-ponder-what-do-golden-ray-n1052216.
11. "Command Vision for US Cyber Command: Achieve and Maintain Cyberspace Superiority" (U.S. Cyber Command, June 14, 2018), 6, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.
12. "Critical Infrastructure Protection, Information Sharing and Cyber Security," U.S. Chamber of Commerce, November 24, 2013, https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security.
13. "The 16 Sectors of Critical Infrastructure Cybersecurity," *Cipher* (blog), October 10, 2017, https://cipher.com/blog/the-16-sectors-of-critical-infrastructure-cybersecurity/.
14. Sarah Nelson, "Report: Local Gov Cyberattacks Reach Critical Level," Government Technology, December 18, 2019, https://www.govtech.com/security/Report-Local-Gov-Cyberattacks-Reach-Critical-Level.html.
15. 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.
16. Mitchell et al., 9.
17. Joseph W. Pfeifer, "Preparing for Cyber Incidents with Physical Effects," *The Cyber Defense Review* 3, no. 1 (2018): 28.
18. Charlie Mitchell, "'Jack Voltaic': Army Cyber Institute Initiative Seen Driving Security Improvements at City Level," *Inside Cybersecurity,* February 18, 2020, https://insidecybersecurity.com/share/10926.
19. Mitchell et al., 5.
20. Mitchell et al., 29.
21. Mitchell et al., 19.
22. Mitchell et al., 15.
23. Natasha Cohen, "Cyber Incident Response and Resiliency in Cities: How Partnerships Can Be a Force Multiplier," New America, Last Updated on February 21, 2019, 4, https://www.newamerica.org/cybersecurity-initiative/reports/cyber-incident-response-and-resiliency-cities/.
24. "Marine Safety Information Bulletin" (United States Coast Guard, December 16, 2019), 1, https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf.
25. "DEFENDER-Europe 20 Fact Sheet" (U.S. Army Europe, February 2, 2020), 1, https://www.eur.army.mil/Portals/19/documents/DEFENDEREurope/DEFENDEREurope20Factsheet200224.pdf.
26. "TRADOC Pamphlet 525-3-1: The US Army in Multi-Domain Operations 2028" (Training and Doctrine Command, 12/6/22018), vi-vii, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.
27. "The National Security Strategy" (The White House, December 2017), 12, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.