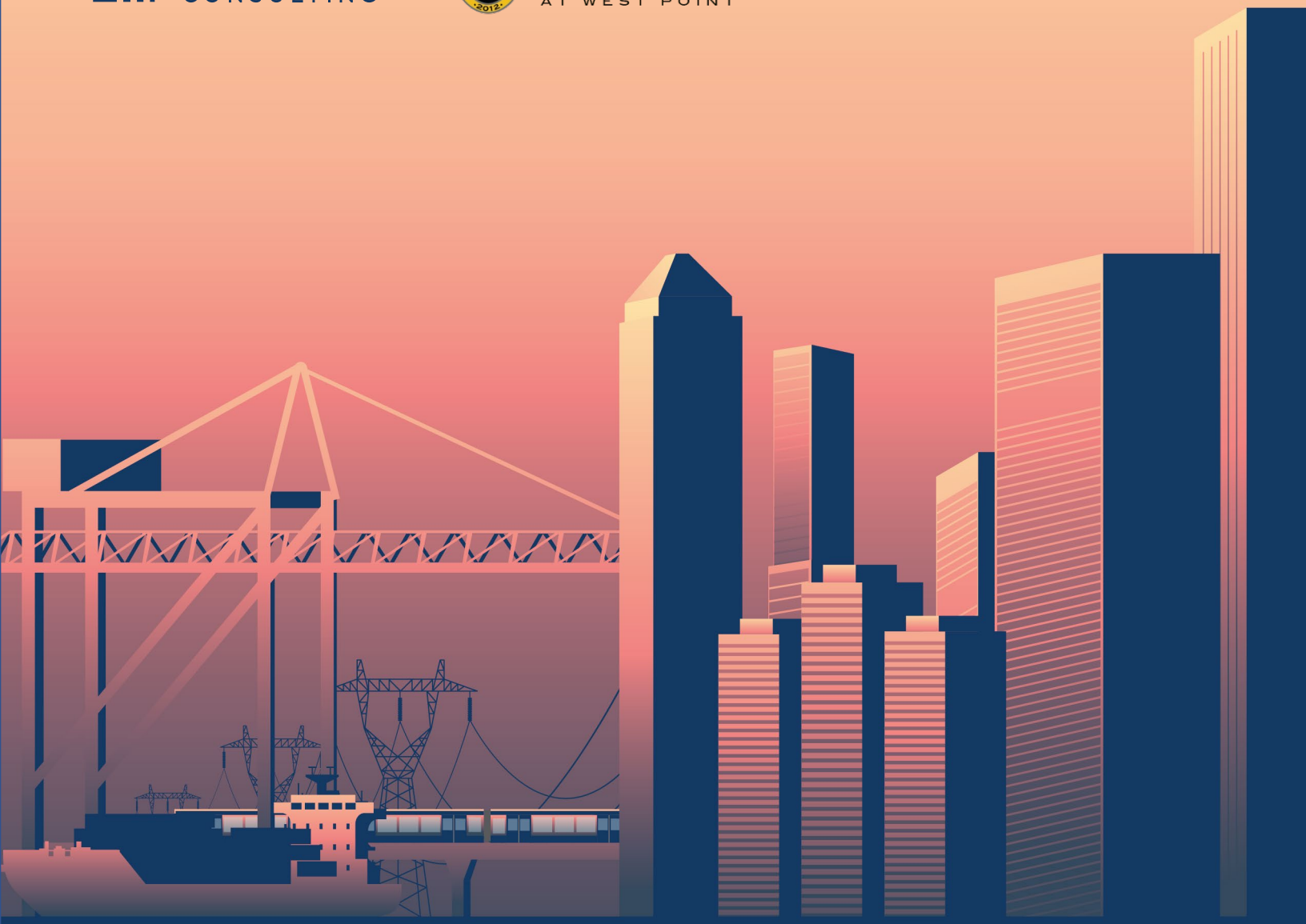
FTI CONSULTING

ARMY CYBER INSTITUTE AT WEST POINT



JACK VOLTAIC 3.0

CYBER RESEARCH PROJECT

BACKGROUND

The critical infrastructure our Federal Government, the Department of Defense (DoD), and our communities rely upon is increasingly connected and potentially vulnerable to cyber attacks. Digital connectivity makes our infrastructure more efficient yet potentially vulnerable – and our reliance on information technology makes cyber disaster response more important than ever.

Infrastructure resilience is critical. The unanticipated impact of a breach could ripple across interconnected infrastructure sectors, and varying defensive capabilities among authorities at the local, state, and national levels complicate the response. If exploited by a determined adversary, these unidentified gaps leave our nation vulnerable. These potential threats and vulnerabilities to critical infrastructure have severe consequences for the DoD's operations, as well as operations for commercial entities, cities and counties.

JACK VOLTAIC 1.0

In 2016 the Army Cyber Institute (ACI), in conjunction with Citigroup, executed a major city, multi-sector, public-private cyber exercise called Jack Voltaic (JV). It was the first step in building a framework to prepare for, prevent, and respond to multi-sector cyber attacks on major cities. Jack Voltaic was a research experiment in the form of a cyber exercise that involved players from multiple sectors, including first responders, emergency management, transportation, telecommunications, power, water, finance and healthcare.

The exercise included two parallel tracks consisting of: 1) an on-range network defender versus attacker live-fire exercise (LFX), and 2) a facilitated table-top exercise (TTX) among sector leadership focused on events occurring in the virtual range play. The goal was to exercise and observe a city's ability, to collaborate in a coordinated respond in any cyber attacks.

JACK VOLTAIC 2.0

The Jack Voltaic 2.0 Cyber Research Project took place July 24-26, 2018, hosted by the City of Houston. Developed by ACI and in partnership with AECOM and Circadence, this research assembled critical infrastructure partners to study cybersecurity and protection gaps in the oil and gas sector.

JV 2.0 explored the employment of the Reserve and the National Guard to defend the Nation by leveraging military cyber capabilities in its domestic response to cyber attacks. Integration of these capabilities allowed participants to gain a better understanding of how policies and legal authorities affect military responses to a cyber attack and develop policy recommendations. Potential gaps in individual skills, training, and equipment were identified to develop best practices. This framework explored how partnerships that leverage the insights and innovations of the public and private sector can enhance Army cyberspace operations.

JACK VOLTAIC 2.5

The objective of the Jack Voltaic 2.5 Cyber Workshop Series was to engage the owners of high-priority DoD, commercial, city and county critical infrastructure as well as municipality leaders on the topic of the key relationships between commercial critical infrastructure and DoD critical missions.

In support of these objectives, AECOM and the Army Cyber Institute, in conjunction with the Department of Homeland Security National Exercise Division, conducted a series of one-day training workshops to share insights from Jack Voltaic 2.0 and discuss how similar efforts have the potential to strengthen the cyber resiliency of DoD missions. These workshops covered the findings and recommendations of the Jack Voltaic 2.0 exercise held in Houston, TX and have helped scope requirements for the Jack Voltaic 3.0 activity in 2020. The workshops took place in Houston, TX; Charleston, SC; Norfolk, VA; Beaumont, TX; Tacoma, WA; San Diego, CA; and Fairfield, CA

JACK PANDEMUS

The Army Cyber Institute, in partnership with FTI Consulting and the Norwich University Applied Research Institute (NUARI) hosted Jack Pandemus, a distributed functional exercise in support of Jack Voltaic® 3.0. This scenario, presented on the DECIDE® platform, explored a gas pipeline disruption caused by a cyber attack, with direct impact to electrical power generation and healthcare delivery. All these events occurred during an ongoing pandemic response.

Jack Pandemus was a remote exercise, using web conferencing technology to cause minimal interruption to the participants daily work schedule while providing a quality venue to exercise critical infrastructure organizations' interdependencies. ACI hosted two separate instances of the same table-top exercise: the June 23, 2020 event focused on the City of Charleston, SC, and the June 30, 2020 event focused on the City of Savannah, GA. Participants can plan on each instance to be a 2-hour, web-based, distributed exercise that they can conduct from their normal work-station.

The Jack Pandemus experiment objectives are to:

- Maintain engagement with the Cities of Charleston and Savannah in preparation for Jack Voltaic 3.0 in September 2020;
- Provide a venue to capture lessons learned from the current pandemic crisis; and
- Demonstrate the use of analytic tools (e.g. Idaho's National Lab All Hazards Assessment) to support better understanding of Community Lifelines, Critical Infrastructure Interdependencies, and Critical Functions.

JACK VOLTAIC 3.0

In partnership with FTI Consulting, the first completely virtual Jack Voltaic™ experiment will take place on 22 and 24 September, 2020, through a regionally focused exercise that includes commercial critical infrastructure supporting military deployment and global logistics operations. Charleston, SC, and Savannah, GA, are key locations that support military force projection. By conducting Jack Voltaic™ 3.0, both cities have an opportunity gain key insights and better understanding of their respective gaps in incident management for a cyber or cyber-enabled disruption or destructive event. Intrepid Networks (via Intrepid Response) is enabling the live mission with communication, coordination, and collaboration features designed for real-live incident management & response.

The Jack Voltaic™ experiment seeks to:

- Affect multiple sectors and require a coordinated local, state, federal, and commercial response;
- Provide a learning environment, using the DECIDE® platform, that enables participants to gain exposure, develop relationships, train, review critical gaps and shortfalls, and assess their response;
- Conduct a virtual "table-top" event where both leadership and technical teams communicate and work within and outside their sectors; and
- Commit to concrete, practical improvements to their resiliency and critical infrastructure preparedness.

The Jack Voltaic™ 3.0 experiment objectives are to:

- Exercise the City of Savannah (in partnership with Savannah Technical College) and City of Charleston (in partnership with The Citadel) in emergency cyber incident response to ensure the fortitude of public services and safeguard critical infrastructure;

- Reinforce a "whole-of-nation" approach and appropriate response to cyber/ physical events through sustained multi-echelon partnership across industry, academia, and government;
- Examine the Army's coordination process for providing cyber protection capabilities on order in support of deployment operations and/or Defense Support of Civil Authorities (DSCA) requests;
- Examine how cyber attacks on commercial critical infrastructure impact Army force projection; and
- Develop a repeatable and adaptable framework that allows a city to exercise their response to a multi-sector cyber event.

ABOUT THE ARMY CYBER INSTITUTE

The Army Cyber Institute confronts the Army's most critical cyber challenges and engages across our government and with our allies to better understand how cyber is changing conflict. ACI was designed with the unique ability to bridge the public and private and to explore challenges through multiple disciplines. This interdisciplinary concept is among ACI's core tenets. The intent is to look for solutions where the Army is not already looking, especially at the strategic and operational levels. For more information, visit https://cyber.army.mil/ and connect with us on Facebook, Twitter, and LinkedIn.

ABOUT FTI CONSULTING

FTI Consulting is a global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting's cybersecurity business is engineered to synthesize cutting-edge, intelligence-led capabilities around a trusted core of comprehensive offerings. This enables clients of any size to address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs to address cyber threats. We build a safer future by helping organizations understand their own environments, harden their defenses, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident. With more than 4,700 employees located in 28 countries, FTI Consulting professionals work closely with clients to anticipate, illuminate and overcome complex business challenges and make the most of opportunities. For more information, visit www.fticonsulting.com and connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.

ABOUT NUARI

NUARI is a 501(c)(3) non-profit that serves the national public interest through the interdisciplinary study of critical national security issues. We are partially funded by the Department of Homeland Security and the Department of Defense, and federally chartered under the sponsorship of Sen. Patrick Leahy. We are co-located with Norwich University in Northfield, VT, and share their ideals of academic excellence, innovation, and service to country. NUARI provides cyber exercises, secure network monitoring, custom consulting, research, and education. We do this through our DECIDE exercises, the Security Situation Center, technology development and deployment, research deliverables, and in-person and online workforce training. For more information, visit www.nuari.net and connect with us on LinkedIn.

ABOUT AT&T

Our first name has always been American, but today you know us as AT&T. We're investing billions into the economy, providing quality jobs to over 200,000 people in the U.S. alone. We're supporting the veterans who make our country stronger and providing disaster relief support to those who need it the most. By bringing together solutions that help protect, serve and connect – committed AT&T professionals are working with the public sector to transform the business of government. www.att.com/publicsector.

ABOUT FIRSTNET

FirstNet is the nationwide communications platform dedicated to America's first responders and public safety community. It's being built with AT&T in public-private partnership with the First Responder Network Authority. FirstNet was born out of the 9/11 Commission recommendations to enhance communications across the entire public safety community. Purpose-built to favor the important work first responders do, FirstNet offers technology, features and functionality designed to properly handle the rigorous, specific and niche demands of first responders. With this much-needed technology upgrade, first responders can connect to the critical information they need every day and in every emergency. Because FirstNet is backed by Congress, it comes with the statutory mandate to help ensure that first responders' needs are met both now and into the future. This allows them to focus on what matters most: serving their communities and saving lives.

ABOUT INTREPID NETWORKS

Our mission is to provide critical operational support to both government and commercial organizations so that team members can instantaneously communicate, collaborate, and coordinate. We provide both standard products for mission and business critical operations as well as custom development for government agencies including development of unique software applications, embedded firmware design, and low-cost communication hardware. Our flagship solution, Intrepid Response, is a FirstNet certified, low-cost, simple-to-use web and mobile situational awareness platform for day-to-day and emergency operations. Mapping, Information Sharing, Team Mobilization, Emergency Notification, and Push-to-Talk voice communications are integrated into an easy to use and deployable solution.

ABOUT SAVANNAH TECHNICAL COLLEGE

Savannah Technical College serves Coastal Georgia with quality, market-driven technical education with campus locations in Chatham, Effingham and Liberty Counties. Serving more than 4,500 credit students each semester, Savannah Tech offers nearly 150 different instructional programs in Aviation Technology, Business and Technology, Public Service, Industrial Technology, and Health Sciences in addition to Adult Education classes, industry-specific training and continuing education. The Cybersecurity Workforce Education Center (CWEC) was launched in 2020 as a multidisciplinary cyber defense education center to meet the growing demands of the National Cybersecurity Workforce shortage and provide training support to municipal and industry partners in the area. CWEC academic education and training for degrees include Computer Support Specialist, Networking Specialist, Cybersecurity and a Cyber Forensics Technology degree is in development. Savannah Technical College has received federal Perkins funding to begin equipping a Cyber Range to support the area cyber workforce training needs. Connect with us at Facebook, Twitter, and LinkedIn.

ABOUT THE CITADEL

The Citadel, with its iconic campus located in Charleston, South Carolina, offers a classic military college education for young men and women focused on leadership excellence and academic distinction. The approximately 2,400 members of the S.C. Corps of Cadets are not required to serve in the military, but about one-third of each class earn commissions to become officers in every branch of U.S. military service. Citadel alumni have served the nation, their states and their communities as principled leaders since 1842. The Citadel Graduate College offers 25 graduate degree programs, 25 graduate certificate programs and 10 undergraduate programs in the evening or online. Named Best Public College in the South by U.S. News & World Report for nine consecutive years and No. 1 Best College for Veterans in the South for two consecutive years. The Citadel is a National Center for Academic Excellence in Cyber Defense Education (CAE-CD) by the National Security Agency and Department of Homeland Security and, in 2016, established the Center for Cyber, Intelligence and Security Studies. The Citadel will offer a new B.S. in Cyber Operations in Fall 2020; minors in Cybersecurity and Cyber Inter-disciplinary Studies are also offered. In 2020, with funding from the National Science Foundation, The Citadel established South Carolina's first CyberCorps Scholarship for Service Program. Connect with The Citadel at Facebook, Twitter, and LinkedIn.