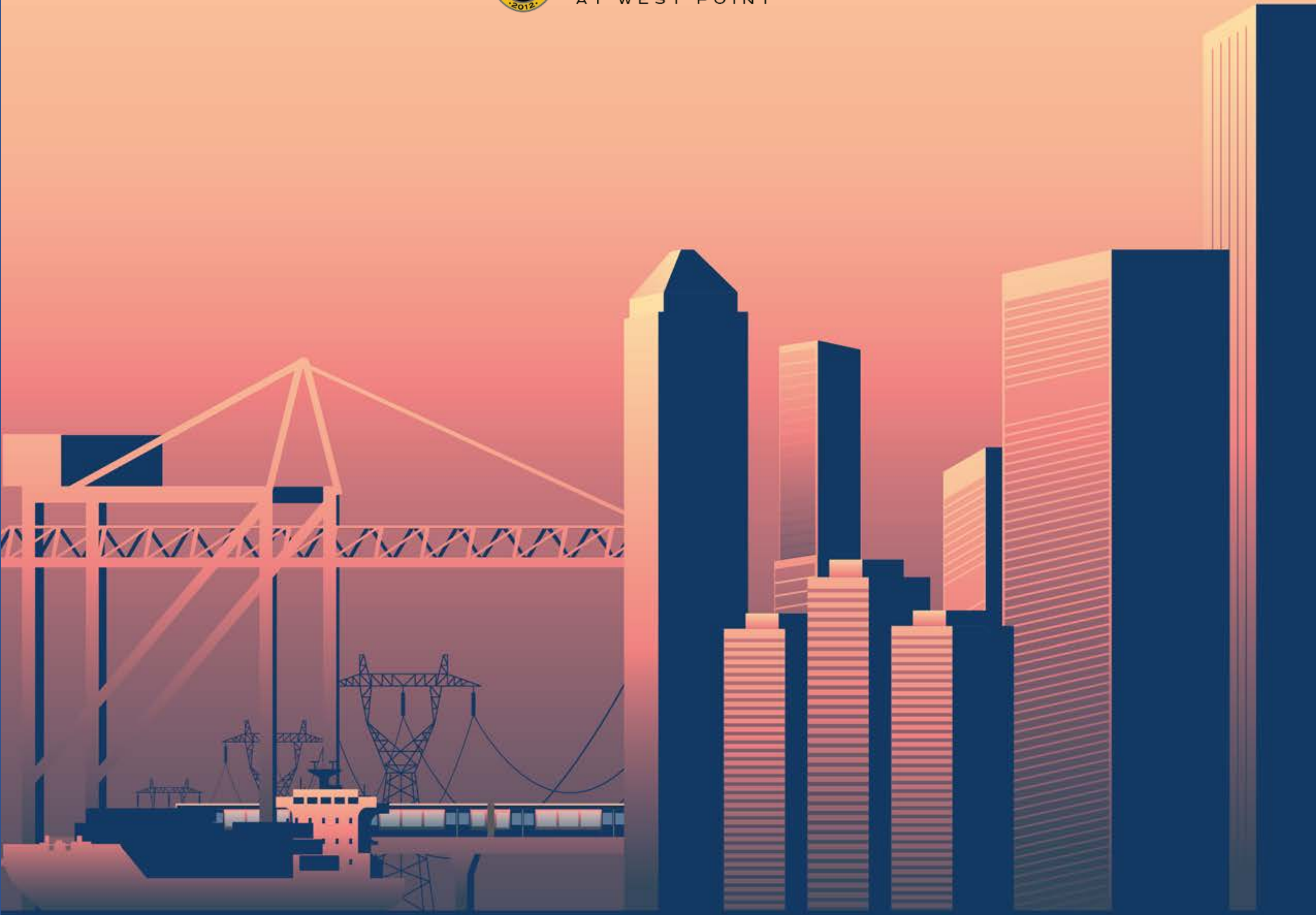
FTI CONSULTING

ARMY CYBER INSTITUTE AT WEST POINT

NUARI



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) will host Jack Pandemus, a distributed functional exercise in support of Jack Voltaic® 3.0. This semi-generic scenario, presented on the DECIDE® platform and using web-conferencing, explores a gas pipeline disruption caused by a cyber attack, which in turn, causes issues with electrical power generation and healthcare delivery. All these events occur during an ongoing pandemic response.

The exercise is designed to cause minimal interruption to the participants daily work schedule while providing a quality venue to exercise interdependencies. We will host two separate instances of the same table-top exercise: the June 23, 2020 event will focus on the City of Charleston, SC, and the June 30, 2020 event will focus 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 and Critical Functions.

JACK VOLTAIC 3.0

The third experiment in the Jack Voltaic™ series, in partnership with FTI Consulting, will take place in 22-24 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.

The Jack Voltaic™ experiment seeks to:

- Affect multiple sectors and require a coordinated local, state, federal, and commercial response;
- Provide a learning environment that enables participants to gain exposure, train, review critical gaps and shortfalls, and assess their response;
- Conduct a synchronized "table-top" and "hands-on-keyboard technical" 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 and City of Charleston 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 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 5,700 employees located in 27 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.