JACK VOLTAIC

conference series

PREPARE | PREVENT | RESPOND | REPORT

ARMY CYBER INSTITUTE AT WEST POINT

NCARI Norwich University Applied Research Institutes

GEORGIA CYBER CENTER AUGUSTA UNIVERSITY

THE CITADEL

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

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 incident 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, the Army Cyber Institute, Department of Homeland Security, and the National Exercise Division conducted a series of one-day training workshops to share insights, findings, and recommendations from Jack Voltaic 2.0 and discuss how similar efforts have the potential to strengthen the cyber resiliency of DoD missions. These workshops helped scope requirements for the Jack Voltaic 3.0 activity in 2020. The workshops took place in San Francisco, CA; Charleston, SC; Norfolk, VA; Augusta, GA; Tacoma, WA; San Diego, CA; and Savannah, GA.

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 were 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 took 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 sought to affect multiple sectors and require a coordinated local, state, federal, and commercial response and 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.

JACK VOLTAIC CONFERENCE SERIES

The Jack Voltaic (JV) Conference Series, conducted in partnership with Norwich University, Georgia Cyber Center, The Citadel, and University of Illinois, will run from June 2021 through May 2022 and consist of four events. The purpose of the JV Conference Series is to share research findings, tools, workshops, and discussions that strengthen critical infrastructure resiliency. The research findings from the JV 3.0 Research Report will be discussed by participants from the exercise, with time for a question and answer session. The JV automated tools will be demonstrated to the audience and audience members will have a chance to try them out, time permitting. There will also be the opportunity to participate in a mini-JV workshop, where participants will work through a shortened scenario built using the automated tools and the DECIDE platform, after which participants will discuss their outcomes. For more information, visit: https://cyber.army.mil/Research/Jack-Voltaic/

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 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 THE NUARI JV CONFERENCE

We are planning a one-day virtual conference that focuses on the new automation technology we are developing in partnership with ACI, 52inc, and Johns Hopkins. We will also be presenting some of the lessons we learned from our participation in JV3. The NUARI Exercise Technology Integration and Cyber Resiliency conference will be held on 23 June from 9am-4pm ET. Some of the topics will include: the integration of MS Teams with the DECIDE platform for more effective distributed tabletop exercises, lessons learned in JV3, master scenario event list construction of effective data analysis, and our development team will demo the new exercise creation automation tool and run through a short exercise using the DECIDE platform.

ABOUT GEORGIA CYBER CENTER

The Georgia Cyber Center at Augusta University is a unique public/private collaboration among academia, state, federal and local government, law enforcement, the U.S. Army and the private sector. Located on the Nathan Deal Campus for Innovation, the GCC is designed to meet the growing need for cybersecurity talent in Georgia, the nation and across the globe. The Georgia Cyber Center is home to certificate, undergraduate and graduate level programs in cybersecurity and cyber sciences. and serves as a hub for technology startups with incubator programs to support cybersecurity and technology innovation and entrepreneurship. Firms and organizations supporting the state's cybersecurity ecosystem can leverage the Center's resources and benefit from the convenience of co-location with state, federal and other industry associates.

ABOUT THE GEORGIA CYBER CENTER JV CONFERENCE

The Georgia Cyber Center will host a two-day conference 9 and 10 November, 2021, specifically focused on critical infrastructure cybersecurity. During the conference we will have experts in the field discussing the current threat landscape and current operational challenges, then highlight current research and other capability development efforts that may help fill some of our current gaps. We will have a deliberate focus on Health IT, the Energy sector, manufacturing and supply chain security and the defense industry.

We will also provide an overview of the Jack Voltaic experiment and the exercise framework they are developing for use by any level of government. It is our intent to provide an after action review of an actual state-level exercise that utilizes the Jack Voltaic exercise framework.

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 has been designated as 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 offers a B.S. in Cyber Operations, undergraduate minors in Cybersecurity and Cyber Inter-disciplinary Studies, and a graduate certificate in Cybersecurity (jointly with College of Charleston). 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.

ABOUT THE CITADEL JV CONFERENCE

The Citadel will host the conference “Cyber Resiliency for Critical Infrastructure” on 24-25 February, 2022. The conference will bring together academic, industry, and government leaders to discuss issues pertaining to critical infrastructure resiliency against cyber threats. The conference will highlight the results of Jack Voltaic 3.0 Execution. The tentative agenda for the conference will include a panel discussion on Cyber Protection for Ports, a panel discussion on Critical Infrastructure Protection against Cyber and non-Cyber Threats, a session on Cyber Risk Assessment for Critical Infrastructure, a mini JV Cyber Table Top Exercise for Critical Infrastructure, a poster session for students presenting their research work on Critical Infrastructure Protection, a session on Cyber Workforce Development. Keynote Speakers will be invited from academia, industry, and government.

ABOUT THE UNIVERSITY OF ILLINOIS / CIRI

The Critical Infrastructure Resilience Institute (CIRI) conducts research and education that enhances the resiliency of the nation's critical infrastructures and the businesses and public entities that own and operate those assets and systems. CIRI is funded by the Department of Homeland Security and is led by the University of Illinois at Urbana-Champaign with collaborators from other U.S. universities and national labs.

ABOUT THE CIRI JV CONFERENCE

The JV 3.0 Concluding Symposium will be held 4-5 May, 2022, in Champaign-Urbana, IL. CIRI and the University of Illinois have a rich portfolio of research and tech transition products that are relevant to the topics that will be discussed at the concluding seminar. A CIRI tool, developed through DHS funds, helps ports assess and measure potential disruptions to their networks. The Cybersecurity Assurance and PRISM tools help analyze risks to critical infrastructures posed by interdependencies and implicit interactions. The University of Illinois also boasts a state-of-the-art advanced electric power grid testbed, funded by DARPA.