Jack Voltaic 2.5

Cyber Workshop Series

Background

The critical infrastructure our Federal Government, the Department of Defense, and our communities rely upon is increasingly connected and potentially vulnerable to cyberattack. Society's reliance on information technology makes cyber disaster response more important than ever. The potential threats and vulnerabilities to critical infrastructure have severe consequences to the DoD in the ability of our nation to apply all of some of its elements of national power.

Infrastructure resilience is more critical than ever. Digital connectivity makes our infrastructure more efficient yet potentially vulnerable. Cyberattacks rarely affect a single target. Instead, unanticipated effects could ripple across interconnected infrastructure sectors. Varying defensive capabilities and authorities complicate the response. If exploited by a determined adversary, these unidentified gaps leave our nation vulnerable.

The Jack Voltaic 2.0 Cyber Research Series is an innovative, bottom-up approach to critical infrastructure resilience. Hosted by the City of Houston in partnership with AECOM and Circadence, the project assembled critical infrastructure partners to study those unidentified gaps. Developed by the Army Cyber Institute at West Point, Jack Voltaic 2.5 Cyber Workshop Series will build our understanding of existing cybersecurity capabilities as well as protection gaps in DoD critical infrastructure security and community resilience. Participants will include DoD critical infrastructure owners along with co-located mayors and city emergency management leads. The focus of these workshops will be placed on visiting communities that directly support DoD's force projection mission.

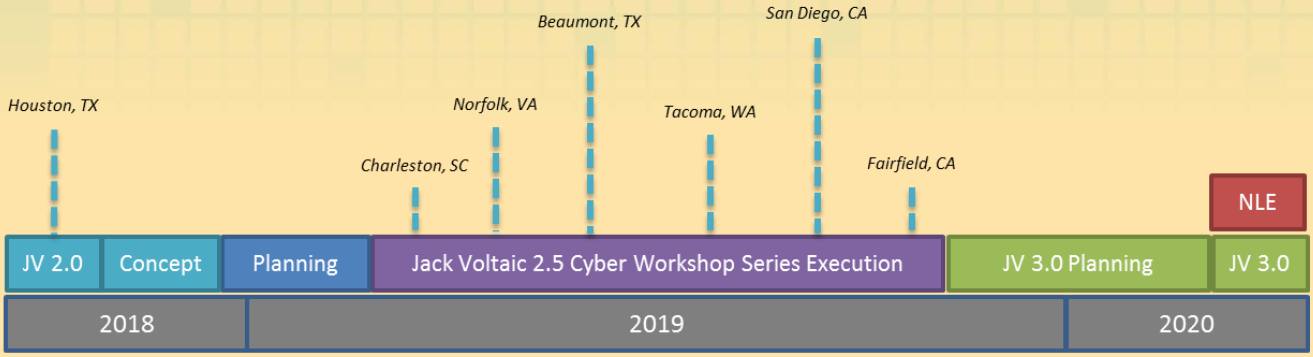
Jack Voltaic 2.5 Cyber Workshop Series Overview

The objective of the Jack Voltaic 2.5 Cyber Workshop Series is to engage the owners of high priority Department of Defense (DoD) critical infrastructure owners 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 will conduct 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 will cover the findings and recommendations of the Jack Voltaic 2.0 exercise held in Houston, TX on 24-26 July, 2018 and help scope requirements for the Jack Voltaic 3.0 activity in 2020.

Prospective Workshop Goals

- Engage the owners of high priority Department of Defense (DoD) critical infrastructure owners and municipality leaders on the topic of the key relationships between commercial critical infrastructure and DoD critical missions
- Disseminate information and educate public and private entities on the lessons learned from the recently conducted Jack Voltaic 2.0.
- Establish wider cyber awareness knowledge base and provide cyber response support information
- Prepare for participation in Jack Voltaic 3.0 and NLE 2020.

Jack Voltaic 2.5 Cyber Workshop Series Timeline



Proposed Presentation Topics

The information below details the proposed topics as well as a notional agenda for each city cyber workshop. Topics provided will include a combination of pre-set presentations and panels that will be provided during each workshop as well as presentations that will be tailored by each city based on their impact on DoD's ability to project power.

Pre-Set Workshop Presentations

1. **Cyber Threat Overview:** Unclassified city-focused presentation covering current cybersecurity risks affiliated with critical infrastructure and national preparedness. Including any vulnerability unique to the representative city.
    - Suggested presenter(s): InfraGard, local fusion center, FBI field Office
2. **Critical Infrastructure Policies and Executive Orders**: Panel members discuss high-level critical infrastructure policies and Executive Orders and how that conveys to municipalities and commercial infrastructure entities identified as DOD critical assets.
    - Suggested presenter(s): Army Cyber Institute, DHS/FEMA
3. **Jack Voltaic 2.0 Lessons Learned:** Presentation discussing the lessons learned during the Jack Voltaic 2.0 Event that took place in the City of Houston, July 24-26, 2018 and what has occurred since.
    - Suggested presenter(s): Army Cyber Institute, AECOM, FEMA, NCICC
4. **Case Study:** Case study of a notional cyber-physical attack, to include: vulnerabilities identified best practices, and follow-on mitigation efforts. Case study will be coordinated with regional DoD entities and the ports they rely on to project power.
    - Suggest presenter(s): Army Cyber Institute, DoD representative(s), AECOM, DHS/FEMA

City-Tailored Workshop Presentations

1. **Information Sharing:** Discussion of information sharing and analysis groups that can be leveraged for specific sectors and augment fusion centers.
    - Suggested presenter(s): AECOM, Army Cyber Institute, DHS/CISA
2. **Additional City-Provided Topics**: Additional topics may be added for each city to align specific DOD goals and outcomes for each workshop.
    - Suggested presenter(s): Topic dependent

Time	Activity
7:00 AM – 8:00 AM	Registration/Check-In
8:00 AM – 8:30 AM	Welcome & Opening Remarks
8:30 AM – 9:30 AM	Topic #1
9:30 AM – 9:45 AM	Break
9:45 AM – 11:00 AM	Topic #2
11:00 AM – 12:45 PM	Lunch
12:45 PM – 1:45 PM	Topic #3
1:45 PM – 2:45 PM	Topic #4
2:45 PM – 3:00 PM	Break
3:00 PM – 4:00 PM	Topic #5
4:00 PM – 4:20 PM	Open Question and Answer Period
4:20 PM – 4:30 PM	Closing remarks
4:30 PM	Adjournment