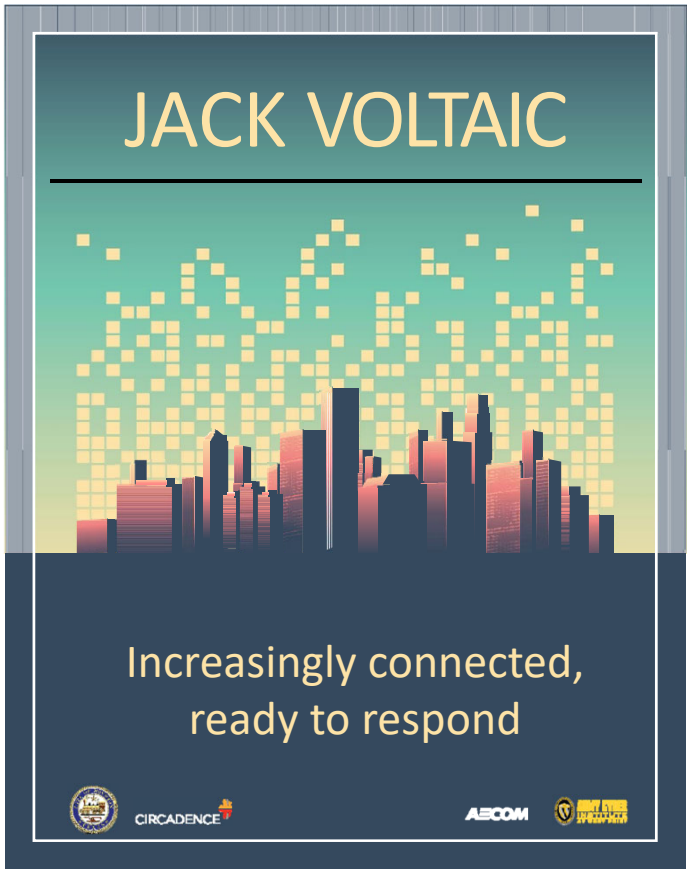
ARMY CYBER INSTITUTE AT WEST POINT




# Jack Voltaic 3.0
# Mid Planning Meeting
# 28-29 Aug 2019

ARMY CYBER INSTITUTE AT WEST POINT

# Jack Voltaic & Defender 2020 Strategy

## What is JACK VOLTAIC?

Focused research on both critical infrastructure and public/private partnerships that explores how to synchronize DoD/USG and private sector capabilities in response to a cyber event.

## What is DEFENDER 2020?

A Department of the Army-directed, U.S. Army Europe led exercise which demonstrates the United States' ability to rapidly deploy a division to the European theater. Deploying units include 1CD (Ft. Hood), 2/1 AD (Ft. Bliss) , 2/3 ID (Ft. Stewart), and 82ABN (Ft. Bragg).

## HOW DO WE USE JACK VOLTAIC TO SUPPORT AND INFORM DEFENDER 2020?

| ENDS | WAYS | MEANS |
|---|---|---|
| Insight into how to synchronize Department of Defense/United States Government, private sector capabilities in a cyberattack response. | Conduct focused research on critical infrastructure and public/private partnerships at the operator, manager, and senior levels. | Execute JV 3.0 in locations (Sannavah, GA; Charleston, SC) supporting force projection of DEFENDER 2020 |

**JACK VOLTAIC 3.0: Examine and analyze the ability of Savannah, GA and Charleston, SC to support force projection in the face of a cyber/information operations attack against critical infrastructure.**

ARMY CYBER INSTITUTE AT WEST POINT

# Jack Voltaic 3.0 Experiment Objectives (DRAFT)

1. Exercise the Cities of Charleston and Savannah in emergency cyber incident response, both for ensuring public services and safeguarding critical infrastructure.

2. Reinforce a “whole-of-community” approach in response to cyber events through sustained multi-echelon partnerships across industry, academia, and government.

3. Examine the coordination process for providing cyber protection capabilities in support of Defense Support of Civil Authorities (DSCA) requests.

4. Develop a repeatable and adaptable framework that allows a city to exercise their response to a multi-sector cyber event.

5. Examine how cyberattacks on civilian critical infrastructure impact Army force projection.

ARMY CYBER INSTITUTE AT WEST POINT

# Work Group Objectives (DRAFT)

1. Test ability to maintain sector's resilience despite systems and communications degradation.
2. Evaluate information sharing processes and procedures
3. When, why, who does a sector need to notify / ask for help?
4. Test effectiveness of current prevention measures, monitoring procedures, response and mitigation techniques, emergency operations procedures
5. Grade / rate readiness to deal with a major cyber incident.
6. Advance awareness of executive leadership on the risks and repercussions associated with cyber incidents.
7. Develop backdoor relationships for training and emergency response assistance.

# Work Group Objectives (DRAFT)

8. Through a combined physical and cyber attack, evaluate local, state, and federal coordination, preparedness, response, and remediation.

9. Evaluate situational awareness, strategic communications, continuity of government, unified communications, logistics tail and service level agreement prioritization.

10. Identify and prioritize (and test priorities where already identified) critical infrastructures that require protection to allow the military force projection to occur unimpeded.

11. Conclusive determination of specific and complete kill chain used in event (including insider threat element).

12. Explore impacts on cyber incident response simulations with period of high system stress and bidirectional impacts with all-hazards electric power system response (up to 72 hrs ahead of cyber boom)

# Work Group Objectives (DRAFT)

13. Identify points of commonality where multiple sectors infrastructure intersect in the physical or logical domains.

14. Identify the platforms used to develop and share common relevant operating pictures.

15. Gain insight on the “pain threshold” to waive which corporate policies to facilitate National Guard and other DoD resources to have logical access to private sector systems to support incident response.

16. Create and execute a scenario where private sector organization requests specific DoD resources and capabilities in support of incident response, and exercise the DSCIR process through actual deployment and employment of DoD resources.

ARMY CYBER INSTITUTE AT WEST POINT

# Jack Voltaic 3.0 Way Ahead