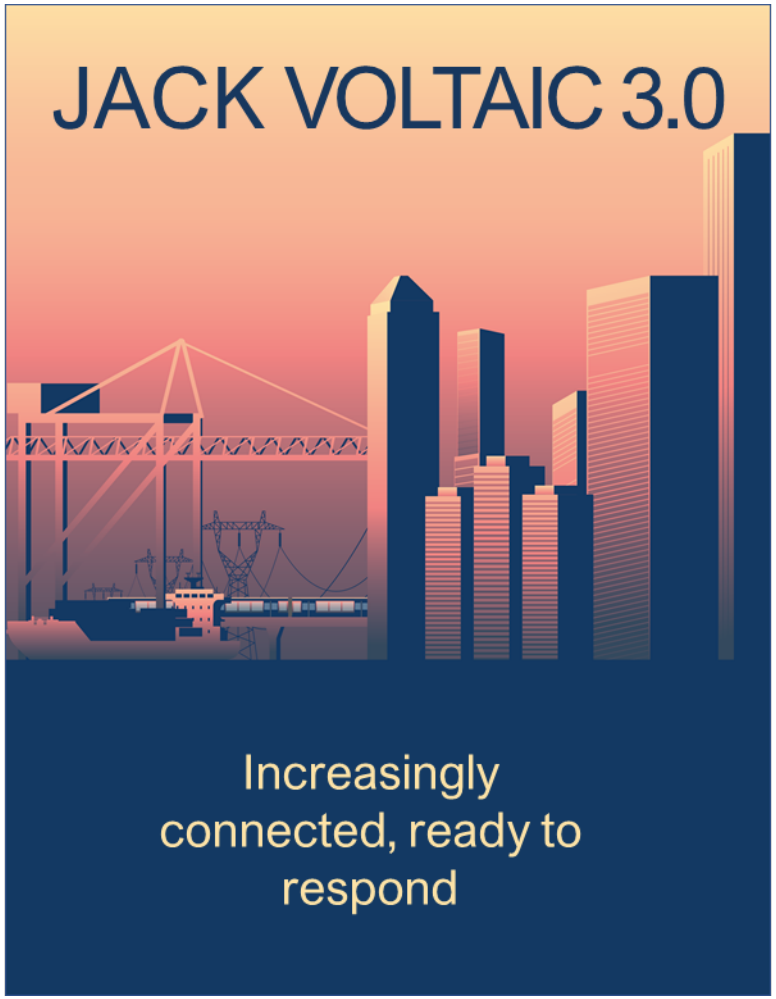


Jack Voltaic Executive Out-brief and Discussion

30 SEP 2020

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 will include sizeable forces from Fort Stewart, Fort Hood, and Fort 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 (Savannah, 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

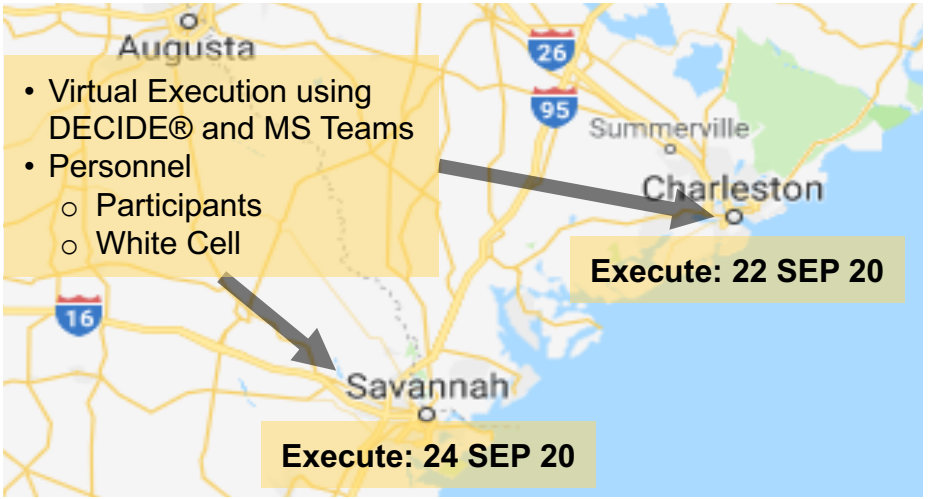
JACK VOLTAIC™ 3.0 Concept of Execution

MISSION: The ACI and their partners *will leverage technology* to execute JV 3.0 *virtually* the week of 22 - 24 September 2020 in the cities of Charleston, SC, and Savannah, GA, in order to understand how cyber attacks against commercial critical infrastructure impact cyber incident response and Army force projection operations.

OBJECTIVES:

- Examine how cyberattacks on commercial critical infrastructure impact Army force projection.
- Exercise the Cities of Charleston and Savannah in emergency cyber incident response to ensure public services and safeguard critical infrastructure.
- Reinforce a "whole-of-community" approach in response to cyber incidents through sustained multi-echelon partnerships across industry, academia, and government.
- Examine the coordination process for providing cyber protection capabilities in support of DSCA requests.
- Develop a repeatable and adaptable framework that allows a city to exercise their response to a multi-sector cyber event.

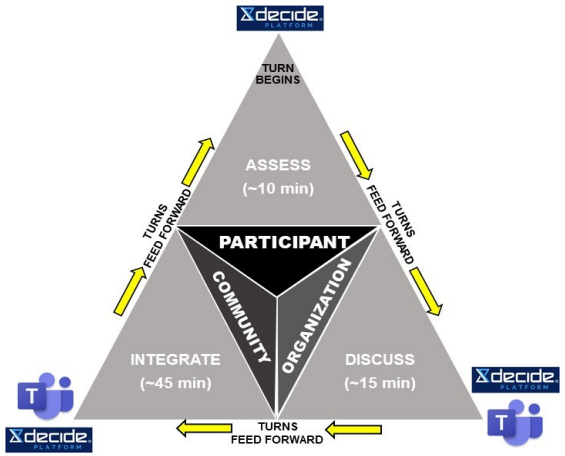
EXECUTION OVERVIEW



- Virtual Execution using DECIDE® and MS Teams
- Personnel
  - Participants
  - White Cell

SEQUENCE OF EVENTS

8:30 am – 9:00 am	Welcome / Scene Setting 0830-0900
9:30 am – 10:00 am	Turn 4 0900-1015
10:30 am	Break
11:00 am – 11:30 am	Turn 5 1025-1140
12:00 pm – 12:30 pm	LUNCH 1140-1240
1:00 pm – 1:30 pm	Turn 6 1245-1400
2:00 pm	Break
2:30 pm – 3:00 pm	Turn 7 1410-1525
3:30 pm – 4:00 pm	Post-Event Survey & AAR



ARMY CYBER INSTITUTE AT WEST POINT

JV 3.0 Participants

Sector	Charleston	Savannah
Transportation	SC Port Authority	GA Port Authority
	Southeastern Freight Lines (Trucking Company)	
	US Coast Guard	
	841st Transportation BN (597th TRANS BDE, SDDC)	
	Charleston Traffic & Transportation	Savannah Airport Commission
Energy	Dominion Energy	Georgia Power / Southern Co.
	Dominion Energy Gas	BP
Emergency Management	SLED	GEMA
	City of Charleston EM	Chatham County EM
	City of Charleston FD	Chatham County PD / 911
	Town of Mount Pleasant EM	City of Savannah EM
		City of Savannah PD & FD
Communications	AT&T (Local Solutions)	
	AT&T Public Sector Solutions (FIRSTNET)	
Information Technology	City of Charleston IT	Chatham County ICS
	Town of Mount Pleasant IT	City of Savannah IT
	DHS CISA Region IV	
Government Facilities	City of Charleston	City of Savannah
	Charleston County School District	Chatham County School District
Water / Wastewater		City of Savannah Water

Additional Participants

GA NG, SC NG, FEMA Region IV, 3ID, USAG Fort Stewart, DoE, ARCYBER, ARNORTH, DCO Region IV, FBI, City of Hinesville, Chubb Insurance, M.C. Dean, Nevada Cyber Solutions, SoCal Gas, Atlas Cybersecurity

White Cell and Research Support

- Norwich University Applied Research Inst.
- Ctr for Army Analysis
- US Army War College
- JHU APL
- Idaho National Labs
- FTI Consulting
- Univ. of Illinois CIRI
- Univ. of South Carolina
- 3rd Infantry Division
- SC Law Enf. Division
- The Citadel
- DISA

Scenario Overview and Intent

- The scenario was intentionally designed to "overcommit" local public and private resources within the cities of Charleston and Savannah.
  - "Real world" examples were utilized to increase realism and believability.
  - "Death by one thousand cuts" meaning, while no single event was catastrophic, the combination of all events could cripple even the most prepared organizations.
  - Reinforce "whole-of-community" approach to cyber critical infrastructure.

- Scenario Overview
  - Heavy rains in Georgia and South Carolina have caused flooding, leading to each Governor declaring a "State of Emergency" and activating elements of the National Guard.
  - United States has publicly announced support for rebelling faction in the Middle East, pledging vehicles, radars, missile systems, and supporting equipment, even some troops.
  - DHS bulletins indicate an increase in malware targeting maritime vessels.
  - Additional reports provide alerts that targeted cyberattacks against the energy and utility sector are expected.

Initial Observations

- PLAN
  - Review planning assumptions & adjust plans related to critical infrastructure protection
  - Review & adjust mitigation strategies—given interdependencies
  - Develop redundant communications and be ready for degraded operations
  - Capture and share best practices
- PREP
  - Ensure “whole-of-government” & “whole-of-community” approach
  - Establish & maintain extensive partner relationships
  - Prepare alternate force projection scenarios

Initial Observations

- EXECUTE
  - Local events can have significant cascading national impacts
  - Gaps in understanding can impact requests for and deployment of state/federal assistance
  - Differences between city, state, federal and private sector responses adds complexity
  - Info sharing and reporting is critical to understanding the situation
- RESOURCE
  - Increase cybersecurity resources for states, cities and CIP
  - Increase training opportunities—leverage tech enablers & a repeatable framework

Critical Infrastructure Research
Potential Ways Ahead

- Complete Final Report
- Provide Advisory Support and Workshops to Select Cities (JV 3.5)
- Continue to Build Out a Repeatable and Adaptable Framework
- Provide Army with Options for Future Events

Back Up

What is Jack Voltaic™?

Scope: A city-focused research event consisting of some combination of table-top exercise and cyber range that utilizes a bottoms-up approach to investigate how cyber-attacks directly and indirectly impact multiple critical infrastructure sectors and the corresponding response from both public and private partners.

Purpose:

- Identify a repeatable and scalable framework usable by any city to rehearse responses to cyber events which affect multiple sectors and require coordinated responses.
- Provide a safe learning environment that enables participants to gain exposure, train, and assess responses to cyber, physical, and cyber-enabled physical incidents.
- Increase communication between leadership and technical teams within their organization and communication between different organizations outside their respective sectors.
- Improve information sharing and response coordination at city, county, and state levels.
- Provide DoD data, information, and feedback to validate planning assumptions and maintain readiness.

Jack Voltaic™ 3.0 Planning Timeline

ARMY CYBER INSTITUTE AT WEST POINT

2019 Key Events

- FEB19: DEFENDER 2020 Planning Conference (Germany)
- MAY19: JV 2.5 (Charleston)
- JUL19: Initial Planning Meeting (Georgia Cyber Center)
- AUG19: JV2.5 and Mid Planning Meeting (Savannah)
- SEP19: Savannah Site Visit
- OCT19: Charleston Site Visit
- DEC19: JV 3.0 OPT Kick-off Webinar

JAN 20 | FEB 20 | MAR 20 | APR 20 | MAY 20 | JUN 20 | JUL 20 | AUG 20 | SEP 20 | OCT 20 | NOV 20 | DEC 20 | JAN 21

13-17 Jan 20: Planner Workshop #1 (S)

17-22 Feb 20: Legal/Policy TTX + PW #2 (S)

03-05 Mar 20: Planner Workshop# 3 (C)

13 Mar 20: DoD issued travel guidance in response to COVID-19

~~**17 Mar 20**~~: Data Collection Workshop

~~**07-09 Apr 20**~~: Rehearsal of Concept + PW #4 (S & C)

~~**28-30 Apr 20**~~: JV 3.0 Execution

16 Mar – 30 Jun 20 DoD Travel Restrictions

01 Jun 20: Hurricane Season Begins

09 Jun 20: Data Analytics Workshop (virtual)

23 and 30 Jun 20: Jack Pandemus TTX (virtual)

07 Jul 20: Data Analytics Workshop (virtual)

09 Jul 20: Update and Way Ahead Webinar (virtual)

21 (C) & 23 (S) Jul 20: Planner Workshop 4 (virtual)

04 Aug 20: Data Analytics Workshop (virtual)

18 (C) & 20 (S) Aug 20: ROC Drill I (virtual)

08 (C) & 10 (S) SEP 20: ROC Drill II(virtual)

22 (C) & 24 (S) Sep 20: JV3 EVENT

30 SEP (C & S): Executive Outbrief and Discussion

Data Post-processing, Report Writing, Project Close-out

Legend

- Event executed IAW original plan
- Event planned but not executed
- Significant event for Cities and ACI
- Planning Challenge

C = Charleston Event
S = Savannah Event

ARMY CYBER INSTITUTE AT WEST POINT

Jack Voltaic 3.0
Scenario Overview by Turn

TURN 1 Mon

Turn 1, set the stage with a series of low impact events that appear to be otherwise unconnected. Initiation of deployment, protests, domestic and APT threat intelligence, security gate failures, admin system issues and a phishing campaign.

TURN 2 Mon

Turn 2, enhance the series of events challenging participants to make connections and communicate across industry lines. Rail manifests failures - cascading delays, power fluctuations, IT requests, validated threats, 911 ghosting begins

TURN 3 Tue

Turn 3 – add layers of complexity (cyber and physical), taxing available resources. Cross industry comms, can the participants connect dots? Loss of shore power, SDDC managing rails delays, LE alert – protests, elevated storm traffic.

TURN 4 Tue

Turn 4 – increase pressure significantly, adding stress on resource availability. Challenge teams to recognize building cross sector issues and cascading impacts. Protests, software and firmware, DoD phishing, threats to utilities.

TURN 5 Tue - Wed

Turn 5 – impact of the building events take effects. Additional suspicious events added increasing heightened state of alert. Coincidence? Violent protests, “ghost calls” + DoS, port and rail security (trespass/obstruction), Mayor’s Office.

TURN 6 Wed

Turn 6 – encourage participants to focus on challenges and move resources effectively amidst growing demonstration of coordinated attack. Protests (attack/dispersed, manual cargo tracking, vessel accident, rail - 2 crude IEDs.

TURN 7 Wed - Thu

Turn 7 – expose growing challenges including verified ransomware in multiple sectors, cascading delays, and human impact of Cyber attack. Final question, is this a coordinated attack? Degraded port OPS, cargo vessel accident, traffic delays, Verified ransomware, power outages.