The Army Cyber Institute

The U.S. Army's Cyber Think Tank

Developing the Critical Capabilities Needed to Respond to Cyber Attacks on US Cities: Jack Voltaic$^{\text{TM}}$ 3.0 Overview

COL Jeff Erickson, U.S. Army
Director
Army Cyber Institute
West Point, New York
jeffrey.erickson@westpoint.edu

How did we get here?

- Historically, civilian infrastructure has been so reliable, military planners have taken the support for granted.

- Similarly, geography and U.S. military dominance has guaranteed security of civilian infrastructure from serious foreign military action.

- The introduction of cyberspace as a domain of warfare often places civilian infrastructure on the front line; the military cannot guarantee similar levels of security.

- Pandemic environment increases greater opportunities for threat actors.

- Response to cyber-attack now relies on multi-layered public/private partnerships, using equally multi-layered application of resources.

Water & Wastewater
Healthcare & Public Health
Government Facilities
Emergency Services
Transportation
Energy
Communications
Defense

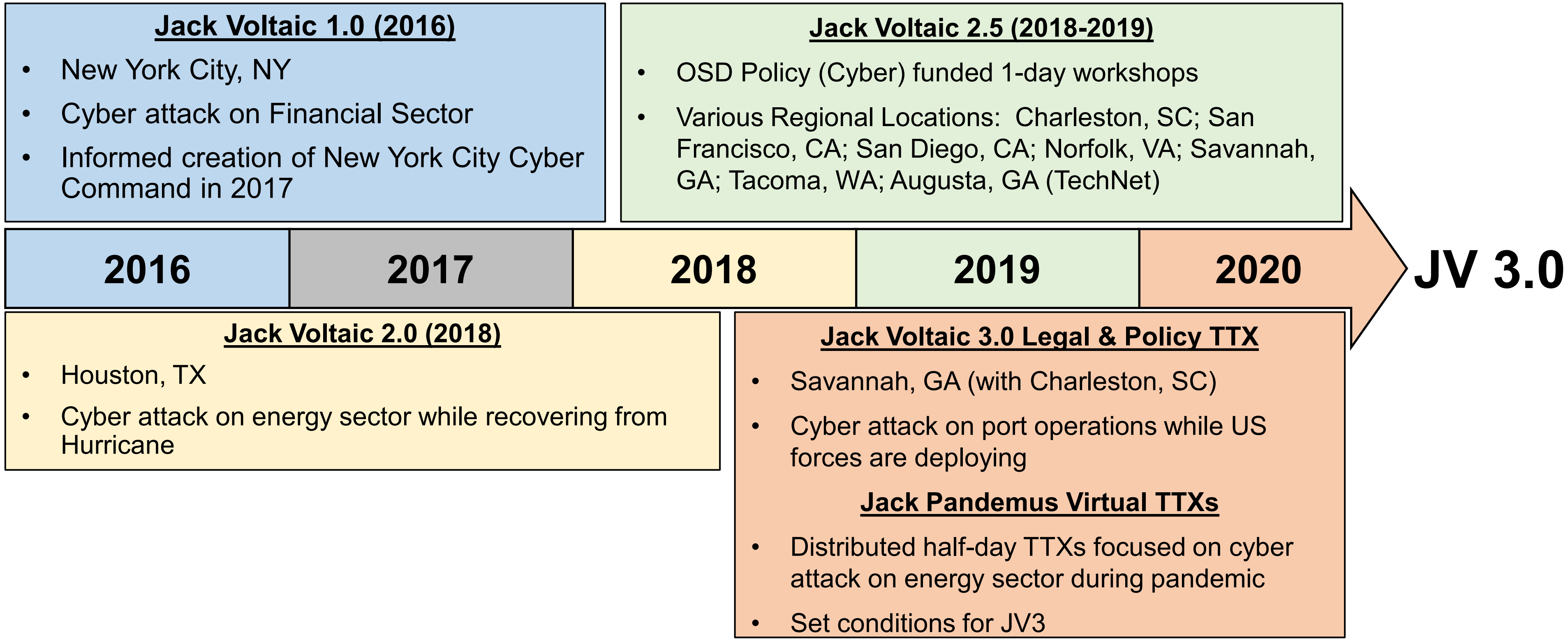
Critical Infrastructure Research: A History of Jack Voltaic^{TM}

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.

GOALS

- Assess a city's response capabilities through a multi-sector cyber exercise at the local level.
- Determine if a city's cyber crisis management planning is sufficiently integrated with physical crisis management planning.
- Develop a repeatable framework for a city's response to a cyberspace attack impacting multiple sectors.



Jack Voltaic 1.0 (2016)

- New York City, NY
- Cyber attack on Financial Sector
- Informed creation of New York City Cyber Command in 2017

Jack Voltaic 2.5 (2018-2019)

- OSD Policy (Cyber) funded 1-day workshops
- Various Regional Locations: Charleston, SC; San Francisco, CA; San Diego, CA; Norfolk, VA; Savannah, GA; Tacoma, WA; Augusta, GA (TechNet)

Jack Voltaic 2.0 (2018)

- Houston, TX
- Cyber attack on energy sector while recovering from Hurricane

Jack Voltaic 3.0 Legal & Policy TTX

- Savannah, GA (with Charleston, SC)
- Cyber attack on port operations while US forces are deploying

Jack Pandemus Virtual TTXs

- Distributed half-day TTXs focused on cyber attack on energy sector during pandemic
- Set conditions for JV3

Jack Voltaic^{TM} 3 Objectives

Jack Voltaic 3.0 Law and Policy
Workshop and Table Top Exercise

1. Examine how cyberattacks on commercial critical infrastructure impact Army force projection.

2. Exercise the Cities of Charleston and Savannah in emergency cyber incident response to ensure public services and safeguard critical infrastructure.

3. Reinforce a "whole-of-community" approach in response to cyber incidents through sustained multi-echelon partnerships across industry, academia, and government.

4. Examine the coordination process for providing external cyber protection capabilities in support of civil authorities.

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

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	
	AT&T Public Sector Solutions (delivering 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

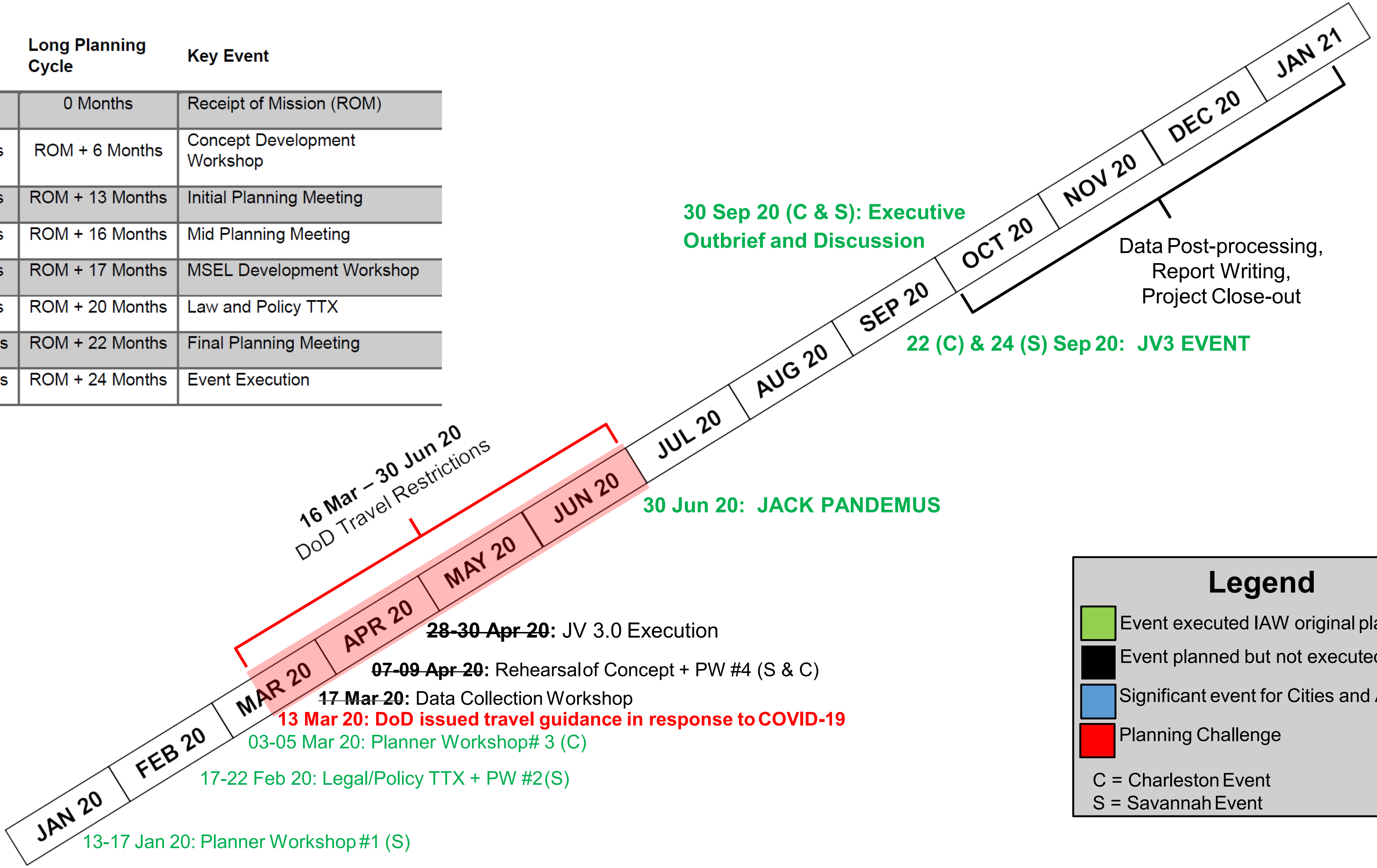
GA NG, SC NG, FEMA Region IV, 3ID, USAG Fort Stewart, DoE, ARCYBER, ARNORTH, DCO Region IV, FBI, City of Hinesville, Chubb Insurance, M.C. Dean, Nevada Cyber Solutions, SoCal Gas, Atlas Cybersecurity

White Cell and Research Support

- Norwich University Applied Research Inst.
- SDDC
- 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
- Savannah Technical College
- Blank Slate Solutions

Jack Voltaic™ 3.0 Planning Timeline

Short Planning Cycle	Mid Planning Cycle	Long Planning Cycle	Key Event
0 Months	0 Months	0 Months	Receipt of Mission (ROM)
ROM + 1 months	ROM + 2 Months	ROM + 6 Months	Concept Development Workshop
	ROM + 4 Months	ROM + 13 Months	Initial Planning Meeting
ROM + 3 months	ROM + 5 Months	ROM + 16 Months	Mid Planning Meeting
	ROM + 7 Months	ROM + 17 Months	MSEL Development Workshop
ROM + 4 months	ROM + 9 Months	ROM + 20 Months	Law and Policy TTX
ROM + 5 months	ROM + 11 Months	ROM + 22 Months	Final Planning Meeting
ROM + 6 months	ROM + 13 Months	ROM + 24 Months	Event Execution



16 Mar – 30 Jun 20
DoD Travel Restrictions

30 Sep 20 (C & S): Executive Outbrief and Discussion

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

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

30 Jun 20: JACK PANDEMUS

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

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

~~17 Mar 20~~: Data Collection Workshop

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

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

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

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

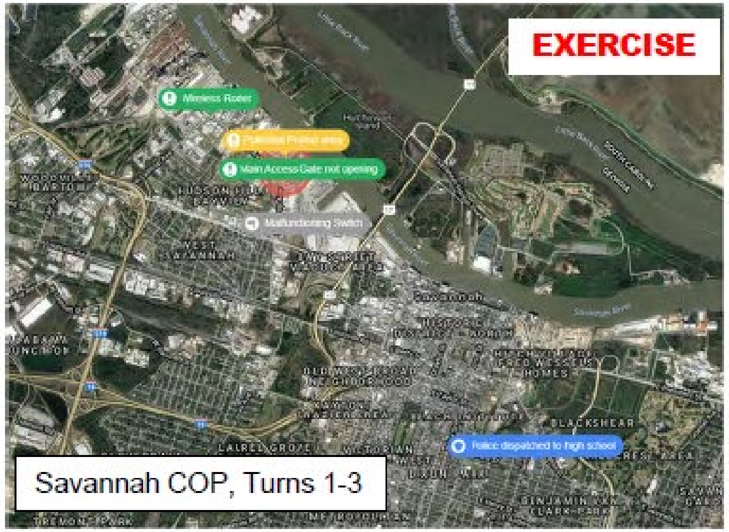
Legend

🟩	Event executed IAW original plan
⬛	Event planned but not executed
🟦	Significant event for Cities and ACI
🟥	Planning Challenge

C = Charleston Event
S = Savannah Event

Scenario Intent and Overview: Savannah

- Cyber intrusions are focused on local municipalities and private industry, not on the US Army.
- Supports both event and participant objectives.
- Intentionally designed to “overcommit” local public and private resources within the cities:
  - “Death by a thousand cuts:” no single catastrophic event.
  - Reinforce “whole-of-community” approach to cyber incident response.
- Maintain realism but introduce ambiguity with respect to cause and / or source of inject.



Savannah COP, Turns 1-3

EXERCISE
Protesters

Savannah COP, Turn 4

EXERCISE
Protesters

Savannah COP, Turn 5

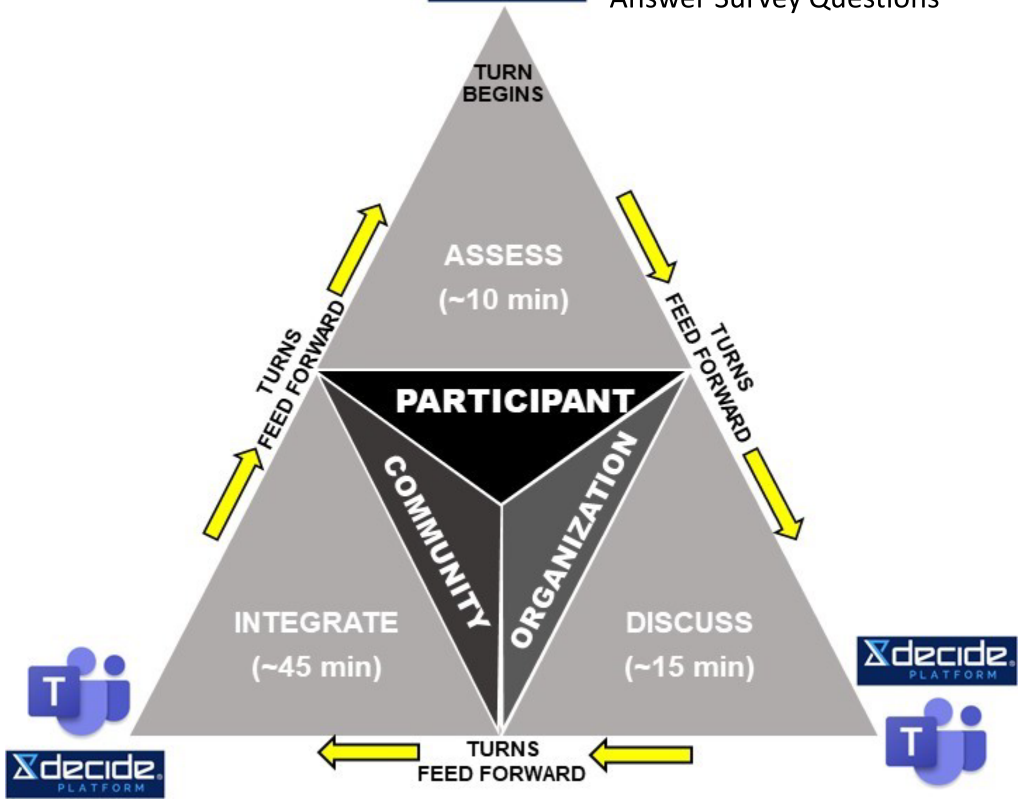
EXERCISE
Protesters
Spill area

Savannah COP, Turn 6

Note: Common Operating Pictures (COPs) provided by Intrepid Networks / Intrepid Response

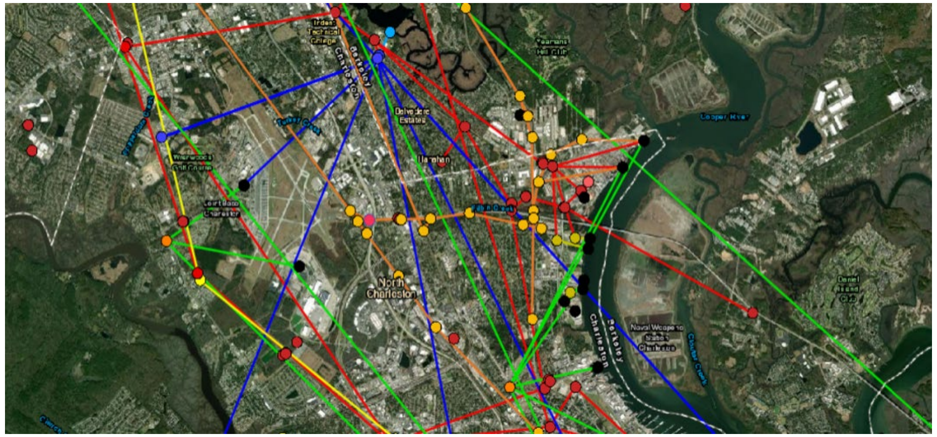
Execution

Individual Email Injects
Answer Survey Questions

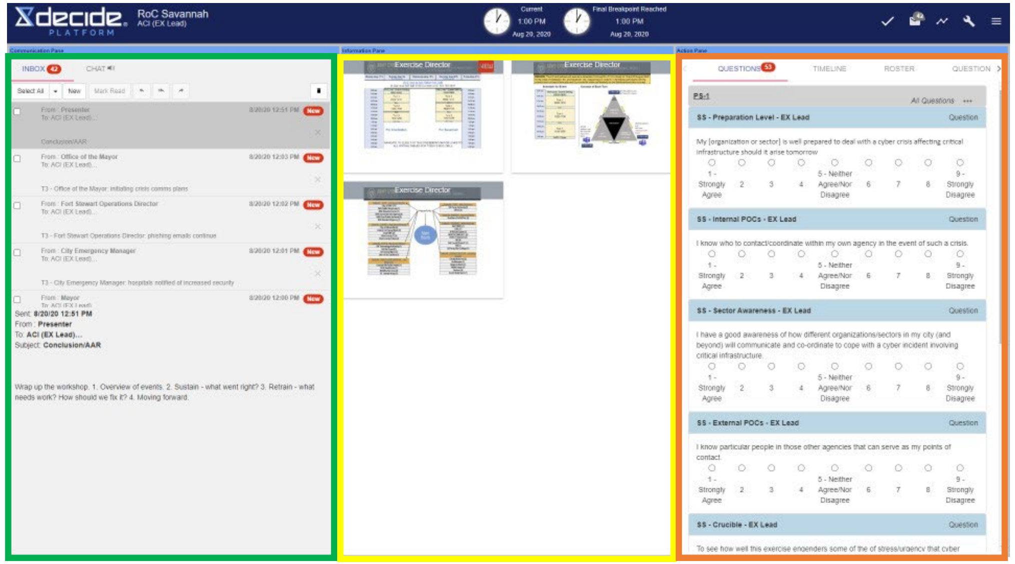


Integrate Findings
Discover Opportunities

Inter-Sector RFI's
Intra-Sector Discussions



Exercise visual from Charleston



RoC Savannah
ACI (EX Lead)

Current
1:00 PM
Aug 20, 2020

Final Breakpoint Reached
1:00 PM
Aug 20, 2020

From : Presenter
To: ACI (EX Lead)...
8/20/20 12:51 PM New
Conclusion/AAR

From : Office of the Mayor
To: ACI (EX Lead)...
8/20/20 12:03 PM New
T3 - Office of the Mayor: initiating crisis comms plans

From : Fort Stewart Operations Director
To: ACI (EX Lead)...
8/20/20 12:02 PM New
T3 - Fort Stewart Operations Director: phishing emails continue

From : City Emergency Manager
To: ACI (EX Lead)...
8/20/20 12:01 PM New
T3 - City Emergency Manager: hospitals notified of increased security

From : Mayor
To: ACI (EX Lead)...
8/20/20 12:00 PM New

Sent: **8/20/20 12:51 PM**
From : **Presenter**
To: **ACI (EX Lead)...**
Subject: **Conclusion/AAR**

Wrap up the workshop. 1. Overview of events. 2. Sustain - what went right? 3. Retrain - what needs work? How should we fix it? 4. Moving forward.

PS-1 All Questions

SS - Preparation Level - EX Lead Question

My [organization or sector] is well prepared to deal with a cyber crisis affecting critical infrastructure should it arise tomorrow

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Internal POCs - EX Lead Question

I know who to contact/coordinate within my own agency in the event of such a crisis.

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Sector Awareness - EX Lead Question

I have a good awareness of how different organizations/sectors in my city (and beyond) will communicate and co-ordinate to cope with a cyber incident involving critical infrastructure.

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - External POCs - EX Lead Question

I know particular people in those other agencies that can serve as my points of contact.

○ 1 - Strongly Agree ○ 2 ○ 3 ○ 4 ○ 5 - Neither Agree/Nor Disagree ○ 6 ○ 7 ○ 8 ○ 9 - Strongly Disagree

SS - Crucible - EX Lead Question

To see how well this exercise engenders some of the of stress/urgency that cyber

Exercise software tool

Summarized Findings

- Force projection can be delayed by a sophisticated adversary without directly targeting military networks or systems.

- While DSCIR has been codified in policy, it has not yet been exercised at the city level and it is unclear how it would work during an incident.

- Demonstrated the value of multi-sector cyber incident response exercises held at the local level.

- Vulnerability to cyber disruption is a “whole of community” problem requiring multi-echelon cooperative action by governmental entities, as well as private industry to solve.

- Incorporating cyber elements into existing exercises should speed the convergence of response maturation and solidify information sharing channels and expectations.

Components of JACK VOLTAIC^{TM} 3.0

- The pie chart shows the different components of a JACK VOLTAIC® event, with the shading representing the distribution of work among the unified team of ACI, committed partners, contracted personnel, and grant-supported research.
- Designing, planning, and executing the JACK VOLTAIC® 3.0 Research Event required the combined efforts of the unified team to achieve all its objectives.

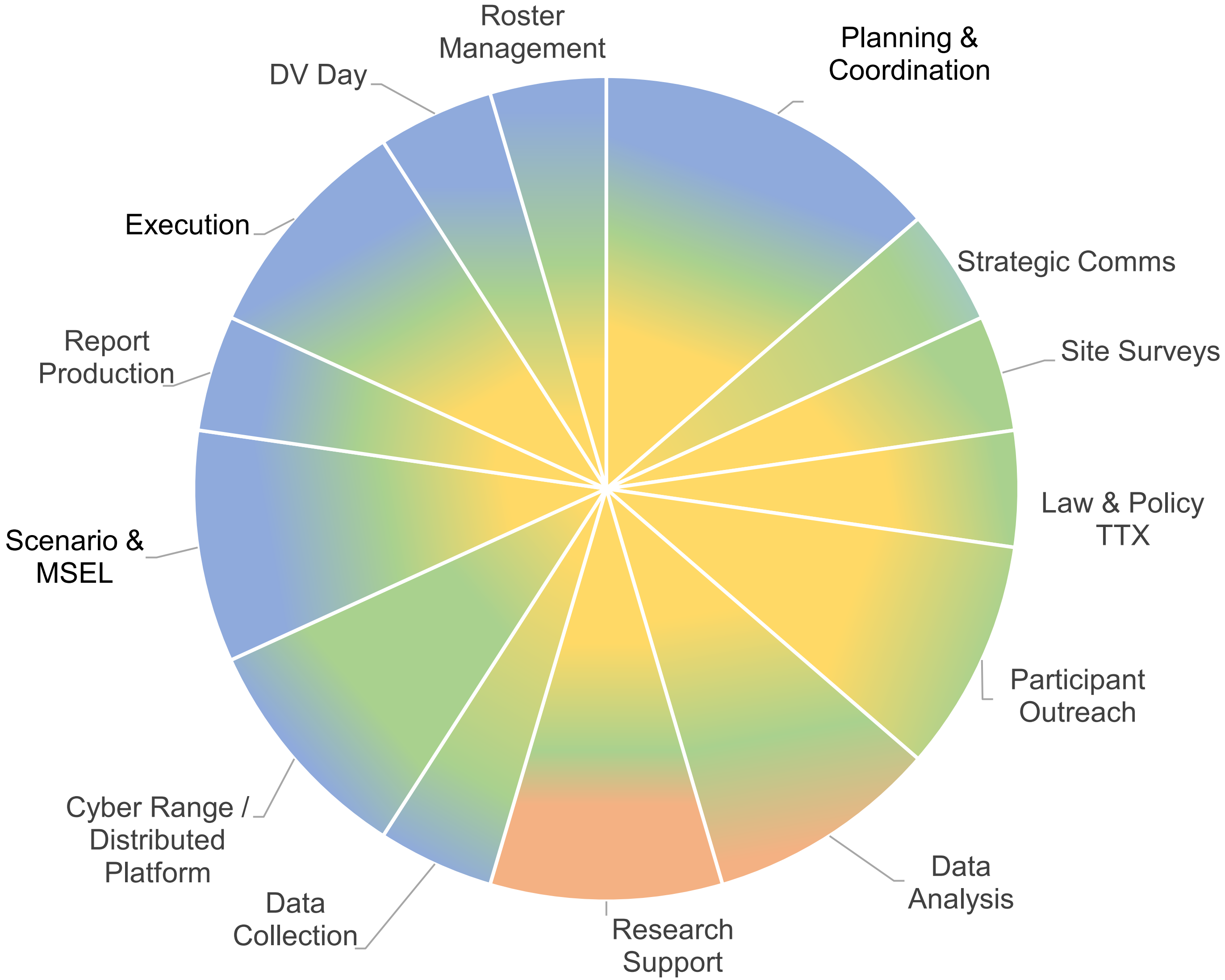


Chart Legend

🟨 ACI
🟦 Contractors
🟩 Partners
🟧 Grant-Supported

Support Documents

- Player Handbook
- Data Collector Guide
- Planning Playbook

SEPTEMBER 11, 2020

JACK VOLTAIC 3.0 PLAYER

22

JACK VOLTAIC™ 3.0

Data Collector Guide

PLANNING PLAYBOOK

Jack Voltaic

Version 1

Approved by:

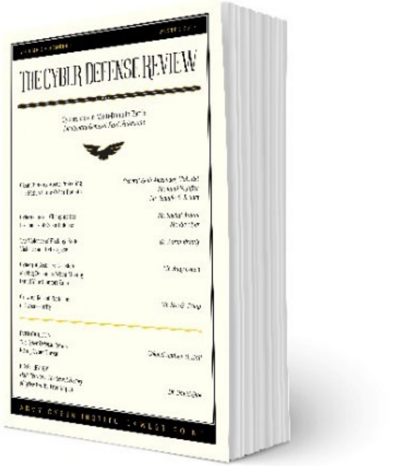
LTC Doug Fletcher, Ph.D
Lead Planner

Things to Consider…

- The demand signals are increasing…who else is working in this space?
- Integration of critical infrastructure aspects into installation or city exercises/events
- Identify solutions for increased use of cyber training environments/ranges
- Build relationships now!

Questions?

Army Cyber Institute
https://cyber.army.mil/



THE CYBER DEFENSE REVIEW

Cyber Defense Review
https://cyberdefensereview.army.mil/

Jack Voltaic^{TM} Research Paper
https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_ResearchReport3.0.pdf?ver=0axzxZB266JjVadSIBTg2g%3d%3d

@ARMYCYBERINSTITUTE @ARMYCYBERINST @THEARMYCYBERINSTITUTE