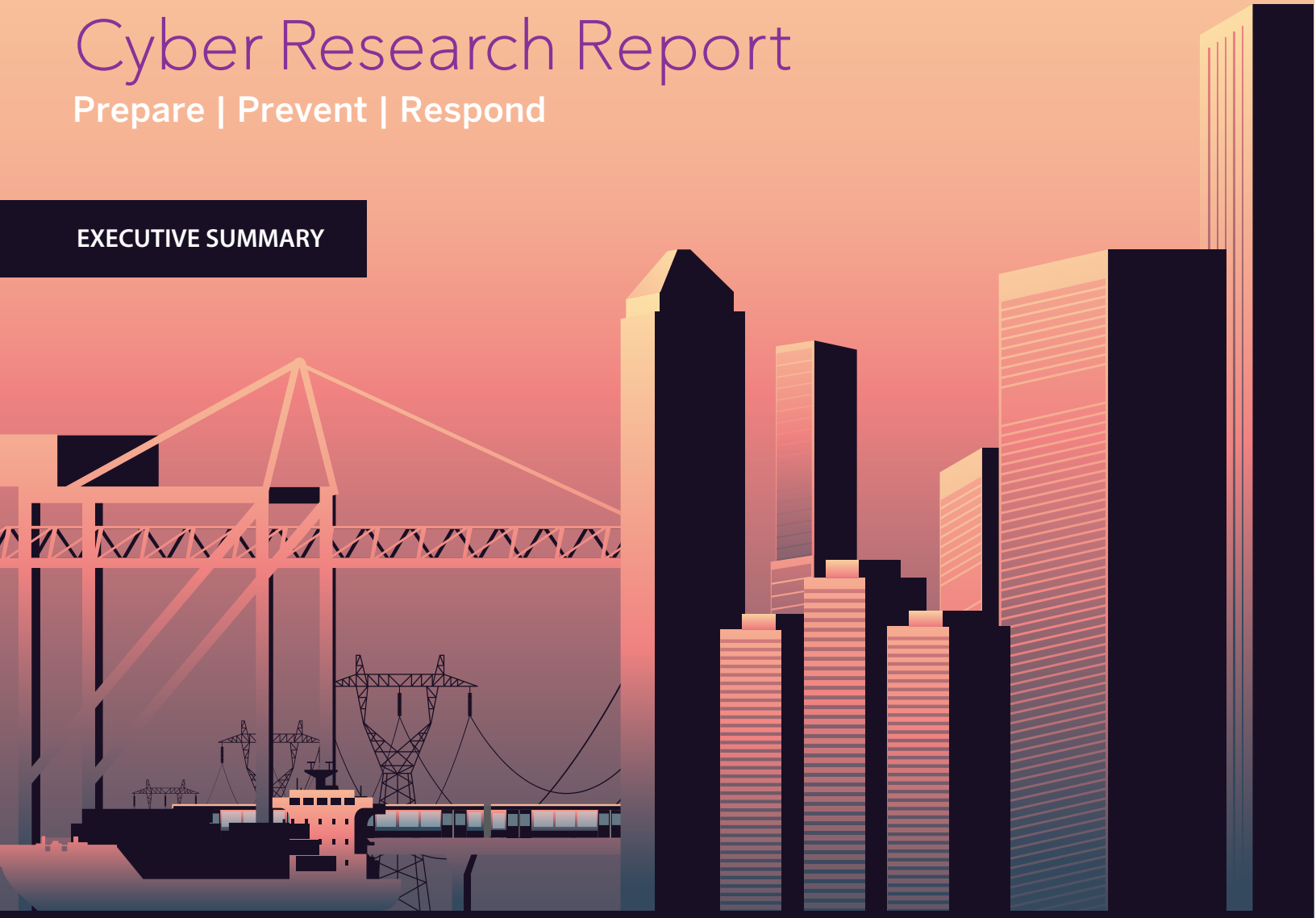
JACK VOLTAIC 3.0

Cyber Research Report

Prepare | Prevent | Respond

EXECUTIVE SUMMARY



Increasingly Connected, Ready to Respond

The Jack Voltaic (JV) Cyber Research Project is an innovative, bottom-up approach to critical infrastructure resilience that informs our understanding of existing cybersecurity capabilities and identifies gaps. JV 3.0 contributed to a repeatable framework cities and municipalities Nationwide can use to prepare. This report on JV 3.0 provides findings and recommendations for the military, federal agencies, and policy makers.

ARMY CYBER INSTITUTE AT WEST POINT

FTI CONSULTING

INTRODUCTION

The Army Cyber Institute's (ACI's) Jack Voltaic (JV) project enables the institute to study incident response gaps alongside assembled partners to identify interdependencies among critical infrastructure and provide recommendations. JV provides an innovative, bottom-up approach to critical infrastructure resilience in two unique ways. Whereas most federal efforts to improve resiliency focus on regional or multistate emergency response, JV focuses on cities and municipalities where critical infrastructure and populations are most heavily populated. Furthermore, JV deviates from other cybersecurity and national preparedness exercises in that it builds around areas of interest nominated by the participants. Although JV events include national-level capabilities and resources, they are conceptually driven by the concerns of the cities and their infrastructure partners. Through this approach, the ACI, the Army, and the Department of Defense (DoD) are able to harvest insights about potential roles, dependencies, partners, and support requests, while cities are able to discover potential capability gaps and expand their critical infrastructure information-sharing networks before a potential disaster strikes.

JV 3.0 leveraged the JV approach to allow the ACI to gain insight into how multiple levels of industry and government respond to a cyberattack against commercial critical infrastructure that supports Army force projection operations—specifically, critical infrastructure in port cities from which Army personnel and equipment would deploy in the case of a military conflict overseas.[1] In parallel with the Army's Defender 2020[2] force projection exercise, JV 3.0 examined and analyzed the ability of Charleston, South Carolina (SC), and Savannah, Georgia (GA)—two major ports on the East Coast—to support force projection in the face of a cyberattack against their commercial critical infrastructure.

Figure 1: JV 3.0 examined and analyzed the ability of Charleston, SC, and Savannah, GA, to support force projection in the face of a cyberattack against their critical infrastructure.

1 Mark Pomerleau, "How the Army Is Strengthening Cyber Cities," Fifth Domain, July 30, 2019, https://www.fifthdomain.com/dod/army/2019/07/30/how-the-army-is-strengthening-cyber-cities/.

2 "DEFENDER-EUROPE 20," Supreme Headquarters Allied Powers Europe (website), n.d., https://shape.nato.int/defender-europe, accessed December 29, 2020.

Originally planned as a 3-day event in April 2020 to be held simultaneously in these two port cities, the ACI decided to make JV 3.0 two single-day, virtual events—one for Charleston on September 22, 2020, and one for Savannah on September 24, 2020—because of complications arising from the coronavirus disease 2019 (COVID-19) pandemic. Leveraging the Distributed Environment for Critical Infrastructure Decision-making Exercise (DECIDE®) platform and Microsoft Teams, the ACI and its partners prepared the participants for the transition to distributed execution through several virtual tabletop exercises (TTXs) and rehearsals that included Jack Pandemus, a half-day event that simulated a cyberattack during pandemic conditions. Table 1 provides information on the different organizations and sectors that participated in and supported JV 3.0.

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, Blank Slate Solution, DCO Region IV, FBI, City of Hinesville, Chubb Insurance, M.C. Dean, Nevada Cyber Solutions, SoCal Gas, Atlas Cybersecurity

White Cell and Research Support:

- Blank Slate Solution
- The Citadel
- DISA
- FTI Consulting
- Idaho National Laboratory
- Intrepid Networks
- JHU APL
- NUARI
- Savannah Technical College
- SLED
- 3ID
- University of Illinois CIRI
- University of South Carolina
- U.S. Army War College

Table 1: JV 3.0 Participants

ORIGIN AND HISTORY OF JACK VOLTAIC

The ACI is an outward-facing partnership think tank of the U.S. Army located in West Point, New York. It began the JV research series to enable the Army's ability to leverage strategic partnerships, to improve information sharing and response at all levels of government, and to develop a repeatable and adaptable framework that local governments can use to rehearse their cyber incident response capabilities. The idea for JV originated from a workshop conducted by the ACI in April 2016 known as the Cyber Mutual Assistance Workshop.[3]

Jack Voltaic 1.0—New York City: The inaugural event, JV 1.0, which was developed with industry partner CITI, examined interdependencies among six critical infrastructure sectors in New York City. The ACI examined these interdependencies by assessing the performance of federal, state, and local governments, as well as private industry, in the event of a Cyber Worst Day scenario.[4]

Jack Voltaic 2.0—Houston: Conducted in August 2018 and developed with industry partner AECOM, JV 2.0 assembled partners from the City of Houston, the State of Texas, federal agencies, and eight different sectors to collaborate on an integrated cyber range and TTX. The event centered on a hypothetical scenario in which a hurricane and cyberspace attack struck simultaneously in and around the Houston region.

Jack Voltaic 2.5—In summer 2019, the ACI held the JV 2.5 Cyber Workshop Series in the port cities of San Diego, Tacoma, San Francisco, Savannah, Charleston, Augusta, and Norfolk. The educational series sought to engage municipality leaders and critical infrastructure sectors to increase cyber awareness and discuss relationships between commercial critical infrastructure and DoD critical missions. AECOM and the ACI, in conjunction with the Department of Homeland Security National Exercise Division, conducted these 1-day training workshops to share insights from JV 2.0 and discuss how similar efforts have the potential to strengthen the cyber resiliency of DoD missions.

SCOPE AND OBJECTIVES

JV 3.0 was a city-focused exercise event that demonstrated how multiple small-scale, cascading cyberattacks against local municipalities and their commercial critical infrastructure in the strategic port cities of Charleston, SC, and Savannah, GA, could disrupt force projection operations. Research objectives included the following:

- Examine the impact of a cyber event on Army force projection;
- Exercise the cities of Charleston and Savannah in emergency cyber incident response to ensure the provision of 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 Defense Support to Civil Authorities (DSCA) requests; and
- Support the development of a repeatable and adaptable framework that allows a city to exercise its response to a multisector cyber event.

3 Jonathon Monken et. al, *Cyber Mutual Assistance Workshop Report* (Pittsburgh: Carnegie Mellon University Software Engineering Institute, 2018).

4 Army Cyber Institute, *Jack Voltaic Executive Summary* (West Point, NY: Army Cyber Institute, 2016).

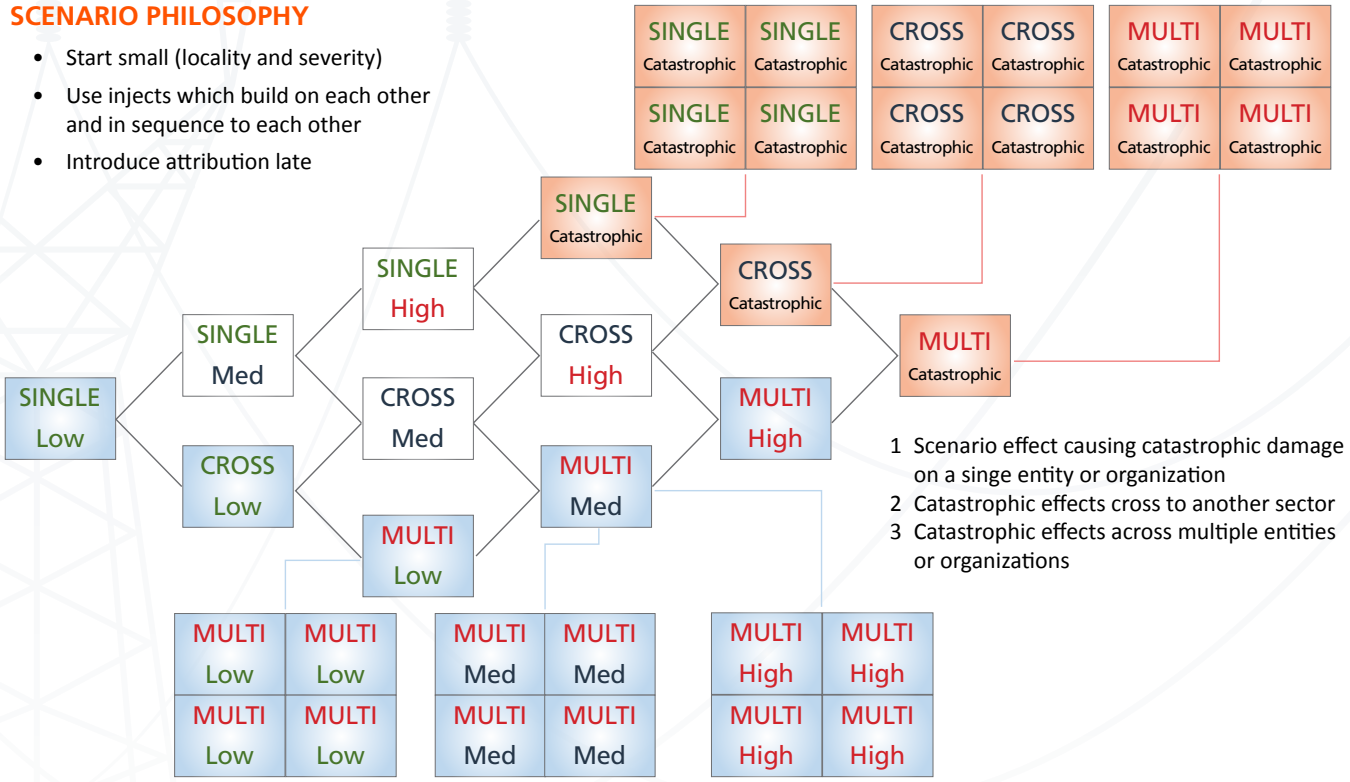
DESIGN CONCEPT

In designing the scenario, the ACI's strategy was to use injects that progressively built upon one another, avoid introducing attribution, and keep incident causes ambiguous for as long as possible. This "death by a thousand cuts" approach allowed the ACI and its partners the opportunity to explore thresholds at which organizations would identify a cyber incident and request support. Keeping the cause of the incident ambiguous facilitated debate among participants, encouraged them to share their decision-making processes with other participants, and increased the realism of the exercise.

The scenario was designed to be played over a series of turns and to weave together multiple independent threads—a set of sector-specific injects that build on themselves—to form a cohesive story. Each thread was built such that its specific injects would grow progressively more dangerous, either by spreading to new areas, organizations, or systems or by causing increased amounts of damage to affected entities. During the planning workshops leading up to JV 3.0, it was evident that many participating organizations, particularly in the municipalities, lacked the resources to adequately defend against a sophisticated adversary. Therefore, the JV Planning Team designed the scenario from a perspective of assumed compromise. Many of the scenario parameters, such as when malware exploitation would migrate from sector to sector, were deliberately kept opaque to the players. This approach forced participants to respond to incidents rather than attempt to defend against them. See figure 2 for a graphical display of the expected progression.

SCENARIO PHILOSOPHY

- Start small (locality and severity)
- Use injects which build on each other and in sequence to each other
- Introduce attribution late



ENTITY	DAMAGE
Single: One organization	**Low:** Internally inconvenient or not noticeable, no noticeable external effect
Cross: Two organizations	**Medium:** Internally disruptive, externally inconvenient
Multi: Three or more	**High:** Internally destructive, externally disruptive
	Catastrophic: Serious economic damage and/or some loss of life, serious disruption or damage to dependent organizations

Figure 2: JV 3.0 Scenario Development Framework

PLANNING TIME LINE

The ACI and its partners held a series of planning meetings and workshops that facilitated establishing the membership of the Planning Committee, understanding stakeholder objectives for the exercise, and developing a scenario that would meet stakeholder and event objectives (see Figure 3, "JV 3.0 Planning Time Line"). Prior to March 2020, the Planning Committee met in person for most meetings and workshops. These on-site events allowed the members of the committee to develop strong relationships and trust that eased the transition to virtual events after pandemic-related restrictions took hold.

When the Planning Committee shifted to a virtual execution, they recognized two key challenges: maintaining stakeholder engagement and increasing participant comfort with the required technology. The ACI, Norwich University Applied Research Institute (NUARI), and FTI Consulting sought to address these challenges by providing stakeholders and participants an opportunity to participate in three separate virtual TTXs. The first, Jack Pandemus, was a 3-hour event that served as a test for virtual execution using both NUARI's DECIDE® and Microsoft Teams. Following Jack Pandemus, the ACI and its partners held two additional 4-hour events using DECIDE® and Microsoft Teams. These rehearsal events allowed the Planning Committee to refine its execution plan and provided participants additional opportunities to gain experience with the event and the various supporting platforms.

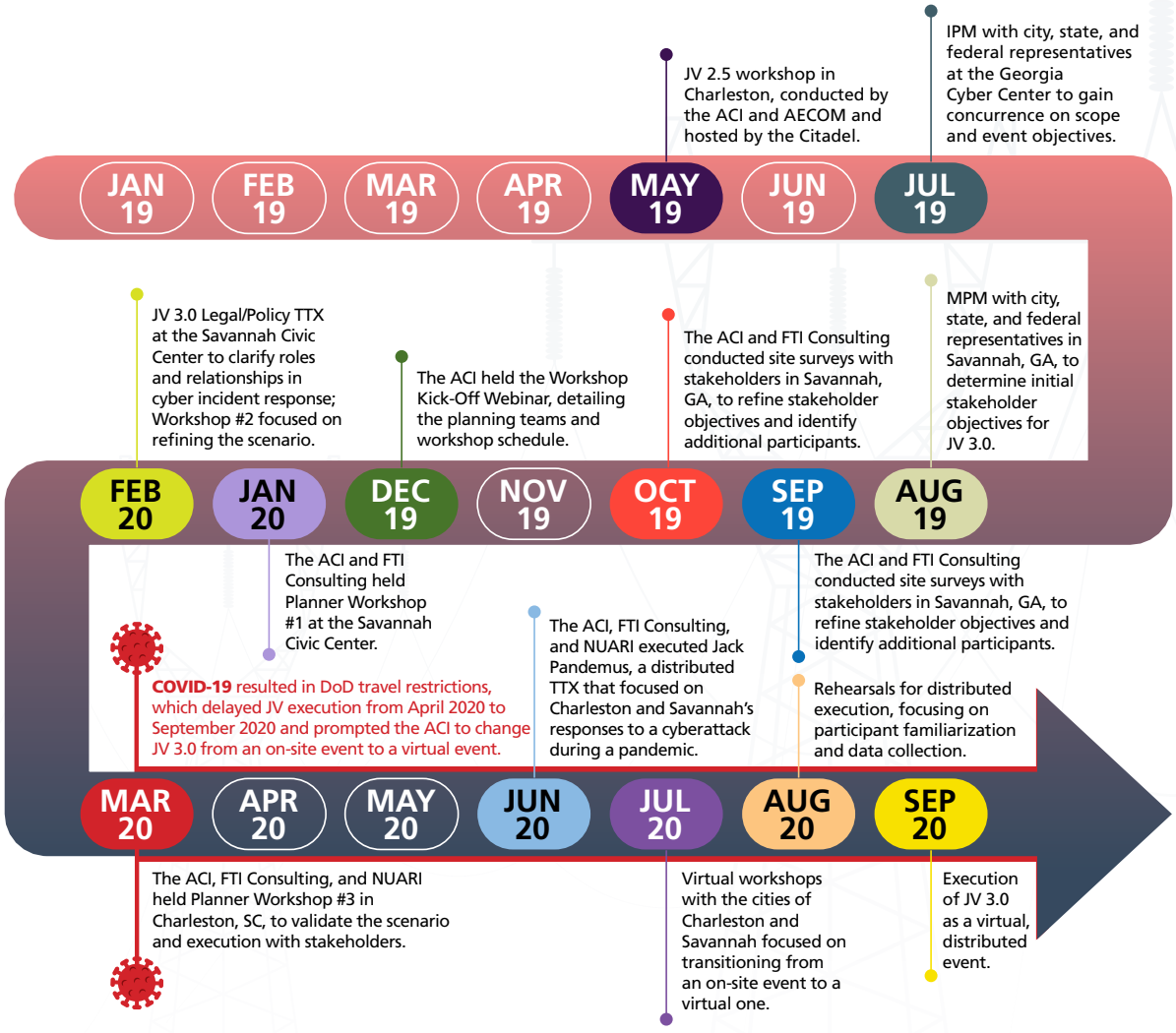


Figure 3: JV 3.0 Planning Time Line

EVENT FORMAT

During each single-day event, participants played the scenario over a series of turns, each of which included three phases. Phase 1, "Assess," allocated approximately 10 minutes for participants to go through their messages in the DECIDE® platform. Within those messages were sector-specific injects as well as messages from other participants (if they had sent any) requesting or supplying information. Phase 2, "Discuss," lasted approximately 15 minutes. In this phase, participants discussed the injects with the other members of their breakout groups. Lastly, Phase 3, "Integrate," lasted approximately 45 minutes and brought all of the breakout groups back into an open forum in which they shared their internal discussions and determined how they would respond to the information provided.

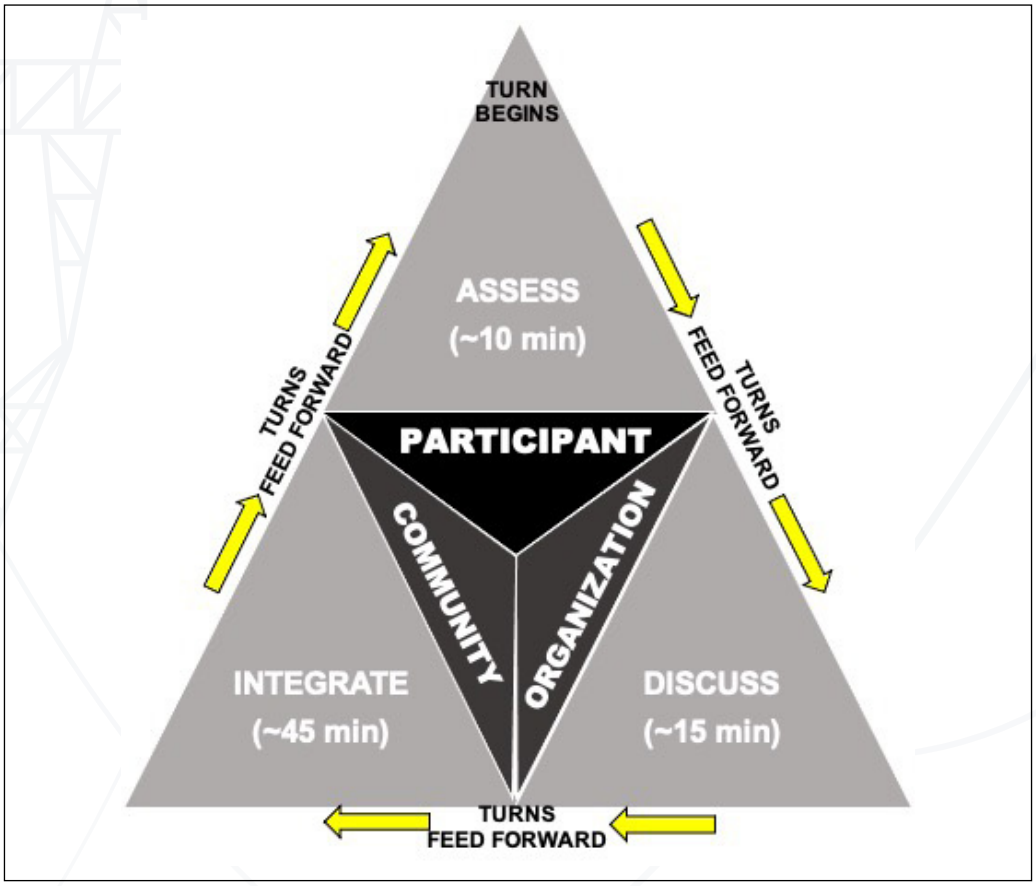


Figure 4: Turn Phases

During each phase, data collectors used the DECIDE® platform to record observations based on their assigned areas.

RESEARCH OBJECTIVES AND FINDINGS

1. Examine the Impact of a Cyber Event on Army Force Projection

    a. The Army relies on various interdependent critical infrastructures, the majority of which it does not own or operate, making its domestic operations heavily reliant on external resources.

    b. A sophisticated adversary can disrupt force deployment and cause units to miss the Required Delivery Date by: (1) targeting commercially owned critical infrastructure and local municipal sectors; or (2) using cyber capabilities that do not trigger an armed response but still achieve cascading effects that complicate a coordinated response.

    c. Interactions and interdependencies between communications and information technology systems present new gray-zone attack vectors that can have debilitating impacts on Maritime Transportation System operations vital to force projection.

    d. The current multidomain environment becomes contested for deploying units as early as the fort, thereby presenting the potential for degraded freedom of maneuver when conducting home-station movement operations. Therefore, military deployment operations can no longer assume such favorable conditions and must plan and prepare for and be ready to mitigate such physical and cyber disruptions accordingly.

2. Exercise the Cities of Charleston and Savannah in Cyber Incident Response

    a. There is no standard for cyber incident declaration. Cyber incident declaration was found to be insufficient in addressing activities that are rated as below catastrophic and are likely not as obvious, yet are still operationally impactful for all parties.

    b. There is an emerging need for city-level information security departments to address potential cross-system issues between organic and isolated networks, such as supervisory control and data acquisition and traffic management systems.

    c. Participants across sectors and levels of government noted that the realistic scenario incidents stressed the participants' procedures and forced them to think differently.

    d. Participants across sectors and different levels of government should use municipality-focused cyber exercises to improve overall incident response.

    e. Municipality-focused cyber and emergency management exercises can be effectively executed in a distributed format that supports continuous participant engagement across both public and private sector stakeholders.

3. Reinforce a Whole-of-Community Approach

    a. Although traditional incident responses—such as for natural disasters or chemical or biological threats—are generally effective and coordinated, there is a need for improving responses to purposeful cyberattacks.

    b. JV 3.0 addressed the need of many participating agencies affiliated with the cities for fully formed response plans and communication networks.

    c. JV 3.0 revealed the need for more regular and codified cross-sector communication and collaboration efforts during cyber incident response.

d. JV 3.0 and the JV series continue to facilitate lasting relationships between a vast array of participating organizations, entities, and sectors.

e. JV 3.0 successfully brought together a wide array of public, private, military, and academic stakeholders during event planning, preparation, and execution for the first time. However, the consensus remains that these new relationships must be continually fostered, and additional stakeholders (those who did not participate in this iteration of JV) must be both identified and incorporated going forward through future, organically driven, JV-like efforts.

4. Examine the Coordination Process for Providing Cyber Protection Capabilities in Support of DSCA

   a. Though Defense Support to Cyber Incident Response (DSCIR) has been codified in policy, it has not yet been exercised, and it is unclear how it would work during an incident.

   b. DSCIR should provide a menu of options and their associated costs similar to DSCA's menu of physical assets.

   c. Whether DSCA or DSCIR is the appropriate mechanism for receiving support in the event of a cyber incident that is beyond the ability of local resources to handle, each municipality needs a clear chain of requests, which could include federal or military resources.

   d. The mechanisms and request chain for the military to request support from their surrounding community ("reverse DSCIR") need to be explored.

5. Support the Development of an Adaptable and Repeatable Framework

   a. Every municipality is different, so it is difficult to develop a "one size fits all" framework.

   b. The Law and Policy TTX is an integral part of the framework requirements due to the challenge of translating national-level laws and policies at the local level and differences in laws and policies across states and localities.

   c. Municipalities do not have the dedicated staff to develop these events internally and will need low- to no-cost assistance to do so.

RECOMMENDATIONS

1. Municipalities should consider adopting new internal incident command structures that enable the formation of tailored whole-of-community efforts consisting of synchronized communication, information sharing, and resource allocation during cyber and emergency incident response.

2. Establish a mentorship program between municipalities that encourages information sharing and joint cybersecurity exercises. The partnership program provides a safe learning environment in which local organizations can further develop their working relationships.

3. Federal, state, and local leaders must recognize cybersecurity and cyber incident response as a key responsibility and allocate resources to personnel, training, and education shortfalls accordingly.

4. State cyber and emergency incident response entities, such as the SC Critical Infrastructure Cybersecurity program within the SC Law Enforcement Division and the Georgia Emergency Management and Homeland Security Agency, should work to establish standing, mutually supportive cyber resource support agreements that utiltize the Emergency Management Assistance Compact framework and Mission Ready Packages to build regionally focused cyber incident response and support plans for responding to a cascading cyber incident.[5]

5. Federal and state entities should execute annual law and policy TTXs that extend to municipalities and private industry. These events provide a venue in which leaders and responders can identify gaps in authorities, rehearse resource requests, and identify potential thresholds. In particular, State and National Guard response authorities and mechanisms differ by state and locality, and these will continue to evolve as cyberspace is better understood. As such, the law and policy TTXs will be critical for understanding the roles and responsibilities associated with utilizing National Guard resources.

6. Federal and state agencies should design and establish a data repository for resources and data related to cyber incidents, tailored responses, impacts, and exercises to facilitate the sharing of policies, procedures, best practices, data, and emerging issues. The repository should be open for municipalities and private entities to deposit and utilize resources to increase the resilience of their associated critical infrastructure.

7. The Department of Homeland Security, in concert with the DoD, should examine and potentially expand the United States Coast Guard Cyber Command's authorizations, resources, and mission set to include initial cyber incident response support for strategic ports and port cities.

8. Through the respective garrisons, U.S. Army Installation Management Command should work to develop, incorporate, resource, and exercise a tailored cyber incident response annex within its emergency incident response plans for force projection and deployment operations.

9. DoD planners must utilize integrated campaigning at multiple echelons (city, county, and state) to understand adversary actions against interorganizational partners and better inform campaign plan assumptions.

10. In conjunction with academic and government partners, the ACI should develop and implement automated tools that will allow novice planners to rapidly design and quickly execute JV-like events.

5 "Emergency Management Assistance Compact," Federal Emergency Management Agency (website), n.d., https://www.fema.gov/pdf/emergency/nrf/EMACoverviewForNRF.pdf.

ACRONYMS

Acronym	Definition
3ID	3rd Infantry Division
ACI	Army Cyber Institute
ARCYBER	United States Army Cyber Command
ARNORTH	U.S. Army North
BDE	Brigade
CIRI	Critical Infrastructure Resilience Institute
CISA	Cybersecurity & Infrastructure Security Agency
COVID-19	Coronavirus disease 2019
DCO	Defense coordinating officer
DECIDE®	Distributed Environment for Critical Infrastructure Decision-making Exercise
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOE	Department of Energy
DSCA	Defense Support to Civil Authorities
DSCIR	Defense Support to Cyber Incident Response
EM	Emergency management
FBI	Federal Bureau of Investigation
FD	Fire department
FEMA	Federal Emergency Management Agency
GA	Georgia
GEMA	GA Emergency Management and Homeland Security Agency
ICS	Industrial control system
IPM	Initial planning meeting
IT	Information technology
JHU APL	Johns Hopkins University Applied Physics Laboratory
JV	Jack Voltaic
MPM	Midplanning meeting
NG	National Guard
NUARI	Norwich University Applied Research Institutes
PD	Police department
SC	South Carolina
SDDC	Military Surface Deployment and Distribution Command
SLED	SC Law Enforcement Division
TRANS	Transportation
TTX	Tabletop exercise
USAG	U.S. Army Garrison

Table 2: Acronyms

cyber.army.mil

@ArmyCyberInst **@ArmyCyberInstitute** **armycyberinstitute** **armycyberinstitute**

For the full report as well as more information on JV, please visit the JV website at https://cyber.army.mil/Research/Jack-Voltaic/