JACK VOLTAIC 3.0
Summary

BACKGROUND

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. In parallel with the Army's Defender 2020 force projection exercise, the ACI partnered with the cities of Charleston, South Carolina, and Savannah, Georgia—two major ports on the East Coast—to conduct JV 3.0 and gain key insights into how multiple levels of industry and government respond to a cyberattack against commercial critical infrastructure that supports Army force projection operations. Originally planned as a 3-day event in April 2020 to be held simultaneously in Charleston and Savannah, the ACI decided to make JV 3.0 two single-day, virtual events—one in Charleston on September 22, 2020, and one in Savannah on September 24, 2020—because of complications arising from the coronavirus disease 2019 (COVID-19) pandemic.

OBJECTIVES

The ACI's 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 requests
- Support the development of a repeatable and adaptable framework that allows a city to exercise its response to a multisector cyber event

SUMMARIZED FINDINGS

1. A sophisticated adversary can delay force projection without directly targeting military networks or systems and without its efforts being recognized as an attack. The risk of a contested homeland and/or contested movement must be addressed and mitigated.
2. Vulnerability to cyber disruption is a whole-of-community problem that requires multi-echelon cooperative action by governmental entities as well as private industry to solve. JV's bottom-up approach focuses this multi-echelon cooperative action on preparing the communities most likely to be targeted.
3. Natural disaster response is more mature than cyber response, especially when a cyber disruption is dispersed across a region or is nebulous or otherwise unclear. Incorporating cyber elements into existing exercises may expedite the convergence of response maturation as well as solidify information-sharing channels and expectations.
4. Cyber incident identification and declaration are delayed, and may not even occur, in cyberattack scenarios that fall below a catastrophic threshold. Proactive development of cyber incident response plans, guidance, and resources may expedite response times and reduce the effect of a cyber disruption.
5. Leveraging technology to conduct exercises and improve the incorporation of cyber elements into exercises can increase flexibility and participation. Distributed exercises can closely simulate normal conditions in which no incident has been declared as well as the emergency operations center environment in which responders are working closely with one another to address an incident.

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