JACK VOLTAIC 2.0

CYBER RESEARCH PROJECT

Prepare | Prevent | Respond

Increasingly connected, ready to respond

The critical infrastructure our communities rely upon is increasingly connected and potentially vulnerable to cyberattack. Society's reliance on information technology makes cyber disaster response more important than ever. Cyberattacks rarely affect a single entity. Instead, effects ripple across infrastructure sectors with unanticipated effects. If exploited by a determined adversary, these unidentified gaps make our residents and resources vulnerable.

Hosted by the City of Houston in partnership with AECOM and representatives of major critical infrastructure sectors, the Jack Voltaic 2.0 Cyber Research Project is an innovative, bottom up approach to public-private research into cyber attacks and critical infrastructure protection. The Army Cyber Institute at West Point created and developed the Jack Voltaic 2.0 concept to drive cyber research. The project will help develop a municipal-level cyber incident response framework and research the integration of local, state, and federal assets into incident response.

The exercise portion is July 24—26 at the Houston Emergency Center. Admittance is limited to invited participants. The Army Cyber Institute will publish a publicly available final technical report in November 2018.

CITY OF HOUSTON TEXAS

More information:

contact.cyber@usma.edu

AECOM

ARMY CYBER INSTITUTE AT WEST POINT

RESEARCH OBJECTIVES

1. Develop a framework to exercise the City of Houston's ability to respond to a multi-sector physical and cyber attack.
2. Exercise and showcase the City of Houston as a state and national leader in cyber incident response.
3. Develop collaboration and coordination procedures between the U.S. Army, including National Guard and Reserves, with municipal and state authorities and local critical infrastructure.

Design Concept

Organizational leaders and technical teams will engage in cross-sector communication to address critical threats in a controlled environment. The exercise includes representations of low, medium, and high-level adversarial threat, leveraging recent world cyber threats, with motivations ranging from political ideology to financial gain. All threats will be simulated on a closed network. No real-world systems will be involved.

Live Fire Exercise

This part of the exercise features an on-range virtual IT network and an OT control system environment to provide exposure and training for a multi-sector audience.

Tabletop Exercise

During this part of the exercise, a facilitator will expertly guide the participants through a discussion based on the exercise scenario. Participants will include essential leaders from local emergency management and responders, supporting critical infrastructure representatives, and the National Guard.

Cyber Exercise Host

The City of Houston

Lead Infrastructure Resilience Advisor

AECOM

Lead Research Advisor

The Army Cyber Institute at West Point

Advisors

Harris County Office of Homeland Security and Emergency Management, The Greater Houston Partnership, Texas State Cybersecurity Coordinator, Texas A&M Cybersecurity Center, The University of Houston.

Critical Infrastructure Sectors

Energy: CenterPoint Energy
Government Facilities: The University of Houston System
Telecommunications: Verizon
Emergency Services: The Houston Office of Emergency Management and the Houston Regional Intelligence Service Center
Healthcare and Public Health: Southeast Texas Regional Advisory Council, Harris Health System, Memorial Hermann Health System, Ben Taub Hospital
Transportation: Port Houston, the U.S. Army Military Surface Deployment and Distribution Command (Port of Beaumont)

CRITICAL INFRASTRUCTURE PROTECTION AND PUBLIC PRIVATE RESEARCH

Jack Voltaic 2.0 will both demonstrate and examine the challenges of responding to two incidents simultaneously and assessing the impact of physical infrastructure degradation on an interconnected, networked environment and vice versa. In the digital age, effectively defending interconnected critical infrastructure requires a whole-of-nation approach, collaboratively undertaken at the local, state, and federal levels. Throughout this research project, the partners have worked together to identify cyber capability gaps and examine how to develop coordinated response strategies and frameworks.

WAY AHEAD

Jack Voltaic 2.0 is an exciting research project with interest from numerous public and private entities. State and local officials are integrated into all aspects of planning and the scenario will play out on a closed network with no access to real-world infrastructure. Federal military personnel will be both participants and observers. No state or federal military forces will be operationally deployed. Due to space constraints and to maintain the research focus, observer and media access will be limited. The Army Cyber Institute will publish the Jack Voltaic 2.0 Technical Report in November 2018, detailing the research project and results and recommendations. This report will help officials prioritize future research and cyberattack preparations. The State of Texas will use this report to develop a statewide cyber response plan. The U.S. Army will use this report to develop its doctrine for providing cyber defense capabilities to civil authorities.

Version 2018.06.12