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

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

Addressing the Situation: Jack Voltaic™

Scope: A research experiment event that demonstrates how cyber-attacks can impact multiple critical infrastructure sectors.

Overall Experiment Purpose: A local government focused experiment in the form of an exercise that looks at a city's ability to respond to a multi-sector cyber-attack.

- Identify a repeatable response framework
- Provide a learning environment
- Focus on information sharing and response coordination

Component 1:
Live-Fire-Exercise (LFX)

Component 2:
Table-Top-Exercise (TTX)

Component 3:
Planning Committee

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.

ARMY CYBER INSTITUTE AT WEST POINT

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

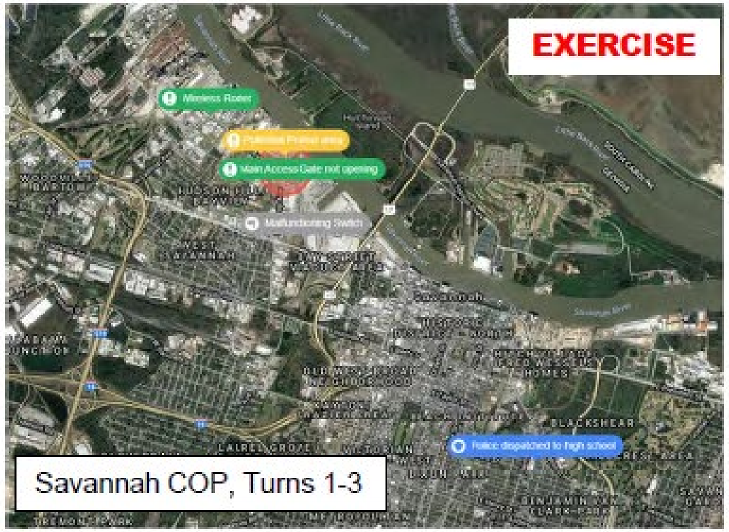
GA NG, SC NG, FEMA Region IV, 3ID, USAG Fort Stewart, DoE, ARCYBER, ARNORTH, DCO Region IV, FBI, City of Hinesville, Chubb Insurance, M.C. Dean, Nevada Cyber Solutions, SoCal Gas, Atlas Cybersecurity

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

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.


EXERCISE
Wireless Router
Main Access Gate not opening
Malfunctioning Switch
Police dispatched to high school
Savannah

Savannah COP, Turns 1-3

EXERCISE
Norfolk RR Line-all clear
Protesters
Norfolk RR Line-all clear
Protesters
Protesters

Savannah COP, Turn 4

EXERCISE
Norfolk RR Line-all clear
Protesters
Norfolk RR Line-all clear
Protesters
Protesters Car Fire
Protesters Car Fire

Savannah COP, Turn 5

EXERCISE
Protests
Spill area
Norfolk RR Line-all clear
Protesters
Norfolk RR Line-all clear
Protesters
Protesters Car Fire

Savannah COP, Turn 6

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

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.

Where do we go from here?

- JV Conferences
  - Georgia Cyber Center (Nov 21)
  - Citadel (Feb 22)
  - University of Illinois Urbana-Champaign (May 22)

- Complete repeatable and automated framework to allow for scaling to more cities

- Integrate critical infrastructure aspects into more Department of Defense exercises/deployments

- Identify solutions for increased use of cyber training environments/ranges

- Build relationships now!

Questions?

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

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

Jack Voltaic™ Research Paper
https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic
_ResearchReport3.0.pdf?ver=0axzxZB266JjVadSIBTg2g%3d%3d

@ARMYCYBERINSTITUTE @ARMYCYBERINST @THEARMYCYBERINSTITUTE