Norwich University Applied Research Institutes

NUARI Technology Integration and Cyber Resilience Symposium

Jack Voltaic 3.0 and NUARI's Distributed Environment for Critical Infrastructure Decision-making Exercises (DECIDE®)

Final Progress Report

Development Report for Grant No. W911NF2010338

Prepared for and Emailed to:
Grants Officer Representative: LTC Christopher Wilkinson, Email: Christopher.wilkinson@westpoint.edu.

Grants Officer: Brandon Hill, Email: s.hill24.civ@mail.mil.

Prepared By:

Norwich University Applied Research Institutes (NUARI)
Philip T. Susmann, President (Principal Investigator)
63 Crescent Avenue, 2nd Floor/PO Box 30, Northfield, Vermont 05663-0030

Contractor Principal Investigator POC: Dr. Kristen Pedersen, Associate Vice President, kpederse@norwich.edu, 802-485-291

Contractor Billing POC: Marlene Betit, CFO, mbetit@norwich.edu, 802485-2009

Authors:

Dr. Kristen Pedersen

DISTRIBUTION A: Approved for Public Release. Distribution is Unlimited.

"Research was sponsored by the United States Military Academy (USMA) and was accomplished under Grant Number W911NF-20-1-0338. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the United States Military Academy (USMA) or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein."

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*
15-11-2021

2. REPORT TYPE
Final Progress Date

3. DATES COVERED *(From - To)*
15-09-2020 to 29-08-2021

4. TITLE AND SUBTITLE
NUARI Technology Integration and Cyber Resilience Symposium - Final Progress Report

5a. CONTRACT NUMBER

5b. GRANT NUMBER
W911NF2010338

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)
Dr. Kristen Pedersen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Norwich University Applied Research Institues (NUARI)
63 Crescent Avenue, 2nd Floor
P.O. Box 30
Northfield, Vermont 05663-0030

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US ARMY ACC-APG-RTP W911NF
800 PARK OFFICE DRIVE
SUITE 4229
RESEARCH TRIANGLE PARK NC 27709

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION A: Approved for Public Release. Distribution is Unlimited.
Research was sponsored by the United States Military Academy (USMA) and was accomplished under Grant Number W911NF-20-1-0338.

13. SUPPLEMENTARY NOTES
The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the United States Military Academy (USMA) or the U.S. Government. The U.S.

14. ABSTRACT
The Army Cyber Institute (ACI) at West Point and Norwich University Applied Research Institutes (NUARI) have closely collaborated since January 2020 to design, create/build, and execute four Jack Voltaic series exercises (Jack Voltaic 3.0 Savannah, Jack Voltaic 3.0 Charleston, Jack Pandemus Savannah, and Jack Pandemus Charleston) using NUARI's team of exercise planners and the Distributed Environment for Critical-infrastructure Decision-making Exercises Platform (DECIDE®). Additionally, ACI and NUARI collaborated with the Johns Hopkins Applied Research Institute and 52inc to develop software for organizations to perform Jack Voltaic-like exercises on their own using an Exercise Scenario Database and Authoring Tool.

15. SUBJECT TERMS
DECIDE, Jack Voltaic 3.0, Distributed Environment for Critical-infrastructure Decision-making Exercises Platform,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Craig Baden
U	U	U	UU	68	19b. TELEPHONE NUMBER *(Include area code)* 802-485-2795

Reset

List of Appendixes

1.0 Summary of Project

The Army Cyber Institute (ACI) at West Point and Norwich University Applied Research Institutes (NUARI) have closely collaborated since January 2020 to design, create/build, and execute four Jack Voltaic series exercises (Jack Voltaic 3.0 Savannah, Jack Voltaic 3.0 Charleston, Jack Pandemus Savannah, and Jack Pandemus Charleston) using NUARI's team of exercise planners and the Distributed Environment for Critical-infrastructure Decision-making Exercises Platform (DECIDE®). Additionally, ACI and NUARI collaborated with the Johns Hopkins Applied Research Institute and 52inc to develop software for organizations to perform Jack Voltaic-like exercises on their own using an Exercise Scenario Database and Authoring Tool.

1.1 Jack Pandemus

The purpose of the Jack Pandemus exercises was to offer a distributed functional cybersecurity exercise to the cities of Charleston, SC and Savannah, GA in support of the upcoming Jack Voltaic 3.0. Both exercises took place in June 2020 and were fully virtual due to COVID-19 restrictions. The cyber-physical exercise scenario was designed to test critical infrastructure organizations' interdependencies during an ongoing pandemic response. The DECIDE® platform allowed for live data capture (via survey questions, chat channels, and data collector input) related to incident response, facilitated the discussion of shared lessons learned during the COVID-19 crisis, as well as demonstrated the use of analytic tools to better understand Community Lifelines and Critical Functions. The resulting data capture of chat channel communications, survey answers, and data collector threads by and between participants and observers in DECIDE® produced valuable information in relation to the Army's coordination process providing cyber protection capabilities in support of deployment operations and global logistics operations.

1.2 Jack Voltaic 3.0

The Jack Voltaic 3.0 exercises (Sept 2020) consisted of two, eight-hour fully distributed exercises that simulated cyber and physical disruptions in the cities of Charleston SC and Savannah GA, testing their ability to defend and respond to multiple threats. Jack Voltaic built upon the data gleaned from the Jack Pandemus exercises and provided a forum to test new knowledge, insights, and lessons learned specifically related to resiliency, critical infrastructure preparedness, and public-private multi-echelon partnerships. The overarching objective was to identify any gaps in response that could impact troop movement and deployment of US troops out of the two ports.

1.3 Exercise Scenario Database and Authoring Tool

One of the fundamental initiatives of the Jack Voltaic series is to build capabilities, processes, and systems that will allow cities, states, and other organizations to perform exercises on their own, outside of Jack Voltaic. To facilitate this effort, NUARI participated in the development of software to integrate DECIDE® with the exercise scenario database created by the University of

South Carolina and 52inc. Integrating the two greatly simplifies the exercise development process, especially for organizations that lack experience but want to run their own exercises. This proof-of-concept integration supported ACI's desire to create an automated process for MSEL creation and direct upload into the DECIDE® platform. To complete the integration, NUARI worked with the developers of the USC application which collects MSEL data to develop a JSON based protocol that allows the transfer of the MSEL data into DECIDE®. Concurrently, NUARI built the software necessary to translate the JSON data into the current DECIDE® supporting database/file system, allowing the scenarios from the USC database to be delivered in typical DECIDE® fashion directly into the platform. Data coming out of the USC database utilizes the concept of branching, or multiple possible outcomes of a scenario, which the data transfer and NUARI's business logic now support. Initial data transfer is in the form of a manual file exchange that contains the exported data in the agreed upon JSON structure. Future iterations of this integration may be developed to automate this data exchange but will most likely utilize the existing underlying JSON format. The second phase (dependent on future funding) of this project will be determined by the amount and type of data being ingested into DECIDE®. In addition to MSEL data, the data transfer could include but is not limited to the sharing of user data, exercise roles, targeting of specific scenario content to specific roles, and questions to present to users during exercise execution.

2.0 Problem: How to disseminate the results from Jack Voltaic 3.0 and provide a proof-of-concept of the exercise authoring tool?

To disseminate the results from Jack Voltaic 3.0, NUARI proposed and received funding to host a one-day research symposium in March of 2021 in Charleston, South Carolina/Savannah, Georgia area. The initial plan to hold the symposium in March 2021 allowed enough time (six months) for post-exercise data analysis and an in-depth after-action review. By January 2021, however, it was clear that an in-person event was not going to be possible due to COVID restrictions, so upon discussion with ACI, NUARI shifted the symposium to a one-day fully virtual format and moved the date to June 2021 to better plan and publicize the event. Three additional institutions proposed their own conferences to complete a total of four Jack Voltaic-specific events spread throughout 2021 and 2022.

As the first in the series of four symposia/conferences, the NUARI event was oriented towards cyber response capabilities as identified during the Jack Voltaic series and the important role of partnerships in a "whole of nation" approach to critical infrastructure resiliency. It was intended to provide a venue for Jack Voltaic information sharing, data presentation, and open discussion of related issues and ideas. A secondary goal was to provide the audience with a Proof-of-Concept demonstration of the Jack Voltaic exercise authoring tool co-developed by ACI, NUARI, Johns Hopkins Applied Physics Laboratory, and 52inc. Both of which were successfully completed. (See Symposium Agenda in Appendix A.)

3.0 Audience

The intended audience of the symposium included previous Jack Voltaic exercise participants, observers/data collectors, partners who helped build and deliver the exercise, senior leadership in all participating organizations, municipal and state government, other interested stakeholders, and anyone who might be a target of opportunity for JV 4.0/5.0 or potentially be interested in using the Exercise Scenario Database and Authoring Tool.

There were 125 registrations through the Eventbrite event registration site. (See Appendix B for full registration list.)

4.0 Marketing

The Symposium was marketed almost entirely through NUARI's website, email campaigns, and social media channels. ACI, the Georgia Cyber Center, the Citadel, and the University of Illinois Critical Infrastructure Research Institute all helped promote the event on their social channels as well. (See Appendix C for examples of social posts.)

5.0 Technology

NUARI utilized MS Teams for the audio and visual elements of the symposium, including dedicated time for online discussion and question/answer sessions between participants and presenters. Additional technology included the exercise authoring tool Proof-of-Concept and the DECIDE® Platform. All of which operated with minimal to no issues.

6.0 Symposium Content and Presentations

Upon completion of the symposium all presentations and videos were made available on the NUARI website and sent as links to all participants. (See Appendix D for the PowerPoint presentations for each session.)

Appendix A – Symposium Agenda

Jack Voltaic Conference Series
Technology Integration and Cyber Resilience
AGENDA
June 23, 2021

ALL Sessions will take place online using MS Teams

9:00 – 9:15 am	**Welcome & Introduction**	**Phil Susmann (President, NUARI)**
9:15 – 9:30 am	**Jack Voltaic 3.0 Background and NUARI Role**	**LTC Erica Mitchell (ACI)**
9:30 – 10:10 am	**Critical Infrastructure and Cyber Resilience**	**Bryson Bort (Scythe)**
10:10 – 10:20 am	**Break**	
10:20 – 11:00 am	**Using Analytic Tools to Identify Critical Infrastructure Dependencies using AHA**	**Tom Muehleisen (NUARI)** **Ryan Hruska (INL)** **MAJ Steve Whitham (ACI)**
11:00 – 11:45 am	**Challenges of Distributed Critical Infrastructure Exercises – Lessons Learned**	**Tom Muehleisen (NUARI)** **Joe Minicucci (NUARI)** **MAJ Steve Whitham (ACI)**
11:45 am – 12:30 pm	**Lunch break**	
12:30 – 2:00 pm	**ACI Technical Integration Project Background & Development Process**	**MAJ Steve Whitham (ACI)** **Mike Schulz (NUARI)** **TR Staake (NUARI)** **Evan Owen (52inc)**
2:00 – 2:10 pm	**Break**	
2:10 – 3:30 pm	**Technical Integration Proof of Concept Demo & Mini Exercise**	**Mike Schulz (NUARI)** **TR Staake (NUARI)** **MAJ Steve Whitham (ACI)**
3:30 – 3:50 pm	**Questions, Discussion, and Feedback**	**Kristen Pedersen (NUARI)**
3:50 - 3:55 pm	**Next Conference: Georgia Cyber Center *Developing a Unified Approach to Critical Infrastructure***	**Eric Toler (GCC)** **MAJ Steve Whitham (ACI)**
3:55 - 4:00 pm	**Closing**	**Kristen Pedersen (NUARI)**

Appendix B – Final Registrant List

First Name	Last Name	Email	Quantity	Attendee Status
Kristen	Pedersen	kpederse@norwich.edu	1	Attending
Jakon	Hays	jhays@norwich.edu	1	Attending
Chris	Tucker	ctucker@norwich.edu	1	Attending
Tom	Muehleisen	tmuehlei@norwich.edu	1	Attending
Filipp	Khosh	fkhosh@norwich.edu	1	Attending
Rachel	Sickler	rsickle1@norwich.edu	1	Attending
Michael	Schulz	mschulz@norwich.edu	1	Attending
Joe	Minicucci	jminicu2@norwich.edu	1	Attending
John	Kunelius	jkuneliu@norwich.edu	1	Attending
Matthew	Bambrick	mjbambrick@me.com	1	Attending
Andrew	Taylor	skida2712@gmail.com	1	Attending
Martin	Eberhardt	eberhardt2@cox.net	1	Attending
Brian	Simmons	cmdrsimm222@gmail.com	1	Attending
Kristin	Hayes	khayes1@norwich.edu	1	Attending
Scott	Gornall	scottg@baonenterprises.com	1	Attending
Lawrence	Furnival	furnival@gmail.com	1	Attending
Filipp	Khosh	fkhosh@norwich.edu	1	Attending
TR	Staake	tstaake@norwich.edu	1	Attending
Eric	Toler	ttoler@augusta.edu	1	Attending
Bill	McConnell	wmcconne@norwich.edu	1	Attending
Philip	Susmann	susmann@norwich.edu	1	Attending
Andrea	Whitesell	whitesel@illinois.edu	1	Attending
Elaina	Buhs	emtucker@illinois.edu	1	Attending
Ryan	Hruska	Ryan.Hruska@inl.gov	1	Attending
Seamus	Leary	sleary@meridianstrategicserv.com	1	Attending
Michael	Lewis	mlewis@ninedss.com	1	Attending
Gabriel	Weaver	gweaver@illinois.edu	1	Attending
Katherine	Balch	kjeden@illinois.edu	1	Attending
Eric	Reid	eric.m.reid@gmail.com	1	Attending
Marcos	Allemand	marcos.allemand@gmail.com	1	Attending
Sameer	Puri	sameer.puri.mil@gmail.com	1	Attending
Eric	Blum	eblum@fti-net.com	1	Attending
Tom	Conway	tom.conway@bluevoyant.com	1	Attending
Whitney	Morris-Reed	sagastrategy@outlook.com	1	Attending
Anthony	Wilcox	spencer.wilcox@pnmresources.com	1	Attending
Ben	Schechter	benjamin.schechter@usnwc.edu	1	Attending

Eric	Meyers	Eric.Meyers@nypa.gov	1	Attending
Brad	Stickles	Bradley.Stickles@jhuapl.edu	1	Attending
Tim	Yardley	yardley@illinois.edu	1	Attending
Ray	Sutliffe II	raysutliffeii@gmail.com	1	Attending
Brandon	Pugh	bpugh@brandonjpugh.com	1	Attending
tony	markel	tony.markel@nrel.gov	1	Attending
Suki	Tsui	sitsui@yahoo.com	1	Attending
Lillian	Isacks	lisacks@grammatech.com	1	Attending
Garrett	Guinivan	garrett.guinivan@gmail.com	1	Attending
COL Scott	Nelson	scott.a.nelson80.mil@mail.mil	1	Attending
Marc	Gilenson	mgilenso@norwich.edu	1	Attending
Peter	Villano	peter.villano@microsoft.com	1	Attending
Ana Nur	Faizah	ananurfaizah@gmail.com	1	Attending
Jeffrey	Morris	jefmorris@augusta.edu	1	Attending
Michael	Nowatkowski	mnowatkowski@augusta.edu	1	Attending
Matthew	Miller	matthew.miller@dal.frb.org	1	Attending
Emile	Bataille	embataille08@gmail.com	1	Attending
Isaac	Porche	ivp5116@arl.psu.edu	1	Attending
Praise	Emiebor	penib4@gmail.com	1	Attending
Jack	Moody	jack.d.moody12.mil@mail.mil	1	Attending
Timothy	Sheard	timothy@sheard.us	1	Attending
Charles	Weissenborn	cweissenborn@dragos.com	1	Attending
Michael	Widmann	michael.widmann@ccdcoe.org	1	Attending
Brian	Lyttle	brian.lyttle@gmail.com	1	Attending
Lawrence	Furnival	furnival@byothermeans.org	1	Attending
Tennille	Scott	nilleybug@yahoo.com	1	Attending
Katherine	Hutton	kar19duke@gmail.com	1	Attending
Gaylon	Caldwell	gcaldwell@orangecountync.gov	1	Attending
Guy	Ashford	guy.ashford@jsou.us	1	Attending
Stefan	Stephenson-Moe	captainnemo001@gmail.com	1	Attending
Dakota	Fitzgerald	walkyourpathinpeace@gmail.com	1	Attending
Jason	Atwell	jason.atwell@fireeye.com	1	Attending
Mona	Stallings	info@mscyrigo.com	1	Attending
John	Reynolds	john.reynolds@fireeye.com	1	Attending
Delmar	Graves	del.graves.dg@gmail.com	1	Attending
Kevin	Kleber	kevin.w.kleber@gmail.com	1	Attending
Diego	Chiza	diegochiza@gmail.com	1	Attending
Rick	Poland	rwpoland@msn.com	1	Attending
BK	Hartzog	bryon.hartzog@jhuapl.edu	1	Attending
Brian	Simmons	cmdrsimm222@gmail.com	1	Attending

Sameer	Puri	sameer.puri.mil@gmail.com	1	Attending
Matt	Lembright	mlembright@censys.io	1	Attending
Ernani	Machado	jmmtech@jmmtech.com.br	1	Attending
Paul	Losiewicz	paul.losiewicz@gmail.com	1	Attending
Dukka	Kc	dukka.kc@wichita.edu	1	Attending
Joshua	Devers	josh_devers@hotmail.com	1	Attending
Michael	Slack	michael.t.slack2.mil@mail.mil	1	Attending
Shankar	Banik	SHANKAR.BANIK@CITADEL.EDU	1	Attending
Eric	Toler	ttoler@augusta.edu	1	Attending
JD	Work	jw3646@columbia.edu	1	Attending
andrew	taylor	skida2712@gmail.com	1	Attending
Clay	Moody	clay.moody@augusta.edu	1	Attending
Bryce	Barros	bcbarros1990@gmail.com	1	Attending
Peter	Wlodarczyk	piotr.s.wlodarczyk.mil@mail.mil	1	Attending
Harry``	Campbell	Harry.Campbell@Savannahga.gov	1	Attending
Warren	Shepard	warren.shepard@gema.ga.gov	1	Attending
Michael	VanPutte	michael.vanputte@provatek.com	1	Attending
Clem	Danish	clemd@blankslatesolution.com	1	Attending
Carey	Lewis	Carey.B.Lewis@uscg.mil	1	Attending
Phil	Owen	phil.owen@mcdean.com	1	Attending
Shawna	Ryan	shawna.ryan@nreca.coop	1	Attending
Martin	Eberhardt	martin.eberhardt@navy.mil	1	Attending
Keith	Jones	keith.m.jones@hq.dhs.gov	1	Attending
Richard	Allen	richard.d.allen56.mil@mail.mil	1	Attending
Aaron	Gould	agould@trideum.com	1	Attending
Vivek	Ponnada	skvpca@gmail.com	1	Attending
Brandon	Grimes	Grimes_brandon@bah.com	1	Attending
Scott	Sanders	ssanders@envistacom.com	1	Attending
Brock	Clary	kyle_clary@charleston.k12.sc.us	1	Attending
Jim	Ruth	jruth@trideum.com	1	Attending
Philip	Niedermair	PNiedermair@wtplaw.com	1	Attending
Tommy	Scroggins	tommy.scroggins@sefl.com	1	Attending
Linda	Riedel	riedell1@citadel.edu	1	Attending
Steven	Steinberg	sstein18@gmail.com	1	Attending
Paul	Wertz	piwertz@gmail.com	1	Attending
Benjamin	Dynkin	ben.dynkin@atlas-cybersecurity.com	1	Attending
Tamekia	Foley	foleytamekia@yahoo.com	1	Attending
Alberto	Rosario	alberto.rosario2.mil@mail.mil	1	Attending
Lyndsey	Burtt	lyndsey.k.burtt.civ@mail.mil	1	Attending
Brian	Kelly	bkelly@educause.edu	1	Attending
Sean	Nikkel	sean.nikkel@digitalshadows.com	1	Attending

Grace	Oh	grace.e.oh@uscg.mil	1	Attending
Paul	Maxwell	paul.maxwell@westpoint.edu	1	Attending
John	Cannady	jcannady@norwich.edu	1	Attending
Chris	Wilkinson	christopher.wilkinson@westpoint.edu	1	Attending
Brendan	Sullivan	Brendan.Sullivan@uscg.mil	1	Attending
Frank	Nein	FrankNein@911Cyber.us	1	Attending
Thomas	Lynch	thomas.lynch@westpoint.edu	1	Attending
Quintin	Sherrod	quintin.sherrod@gmail.com	1	Attending

Appendix C - Website and Social Media Marketing

JACK VOLTAIC

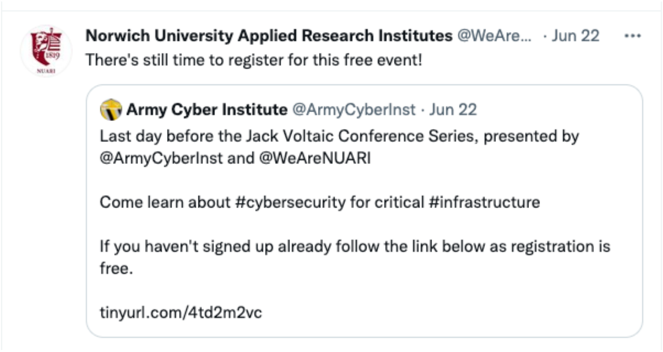
conference series

Prepare | Prevent | Respond | Report

June 23, 2021

Technology Integration and Cyber Resilience

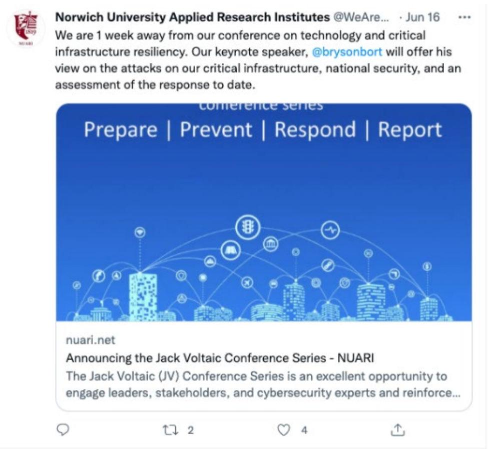
NUARI
Norwich University Applied Research Institutes
THE CITADEL
ARMY CYBER INSTITUTE AT WEST POINT
GEORGIA CYBER CENTER
AUGUSTA UNIVERSITY
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN



Norwich University Applied Research Institutes @WeAre... · Jun 22

There's still time to register for this free event!

> **Army Cyber Institute** @ArmyCyberInst · Jun 22
>
> Last day before the Jack Voltaic Conference Series, presented by @ArmyCyberInst and @WeAreNUARI
>
> Come learn about #cybersecurity for critical #infrastructure
>
> If you haven't signed up already follow the link below as registration is free.
>
> tinyurl.com/4td2m2vc



Norwich University Applied Research Institutes @WeAre... · Jun 16

We are 1 week away from our conference on technology and critical infrastructure resiliency. Our keynote speaker, @brysonbort will offer his view on the attacks on our critical infrastructure, national security, and an assessment of the response to date.

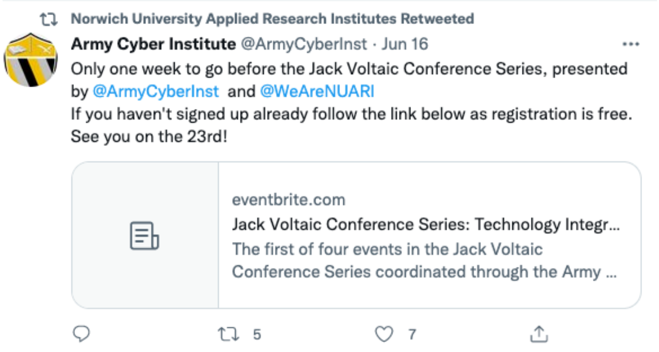
conference series

Prepare | Prevent | Respond | Report

nuari.net

Announcing the Jack Voltaic Conference Series - NUARI

The Jack Voltaic (JV) Conference Series is an excellent opportunity to engage leaders, stakeholders, and cybersecurity experts and reinforce...



Norwich University Applied Research Institutes Retweeted

Army Cyber Institute @ArmyCyberInst · Jun 16

Only one week to go before the Jack Voltaic Conference Series, presented by @ArmyCyberInst and @WeAreNUARI

If you haven't signed up already follow the link below as registration is free.

See you on the 23rd!

eventbrite.com

Jack Voltaic Conference Series: Technology Integr...

The first of four events in the Jack Voltaic Conference Series coordinated through the Army ...

Appendix D – PowerPoint Presentation

JACK VOLTAIC

conference series

Prepare | Prevent | Respond | Report

June 23, 2021

Technology Integration and Cyber Resilience

NUARI 1819
Norwich University Applied Research Institutes

THE CITADEL

ARMY CYBER INSTITUTE AT WEST POINT

GEORGIA CYBER CENTER
AUGUSTA UNIVERSITY

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Welcome to the Conference

9:00 – 9:15 am	Welcome & Introduction	Phil Sussman (President, NUARI)
9:15 – 9:30 am	Jack Voltaic 3.0 Background and NUARI Role	LTC Erica Mitchell (ACI)
9:30 – 10:10 am	Critical Infrastructure and Cyber Resilience	Bryson Bort (Scythe)
10:10 – 10:20 am	Break	
10:20 – 11:00 am	Using Analytic Tools to Identify Critical Infrastructure Dependencies using AHA	Tom Muehleisen (NUARI) Ryan Hruska (INL) MAJ Steve Whitham (ACI)
11:00 – 11:45 am	Challenges of Distributed Critical Infrastructure Exercises – Lessons Learned	Tom Muehleisen (NUARI) Joe Minicucci (NUARI) MAJ Steve Whitham (ACI)
11:45 am – 12:30 pm	Lunch break	
12:30 – 2:00 pm	ACI Technical Integration Project Background and Development Process	MAJ Steve Whitham (ACI) Mike Schulz (NUARI) TR Staake (NUARI) Evan Owen (52inc)
2:00 – 2:10 pm	Break	
2:10 – 3:30 pm	Technical Integration Proof of Concept Demo & Mini Exercise	Mike Schulz (NUARI) TR Staake (NUARI) MAJ Steve Whitham (ACI)
3:30 – 3:50 pm	Questions, Discussion, and Feedback	Kristen Pedersen (NUARI)
3:50 - 3:55 pm	Next Conference: Georgia Cyber Center - **Developing a Unified Approach to Critical Infrastructure**	Eric Toler (GCC) MAJ Steve Whitham (ACI)
3:55 - 4:00 pm	Closing	Kristen Pedersen (NUARI)

Phil Susmann, President, NUARI

NUARI 1819

Norwich University Applied Research Institutes

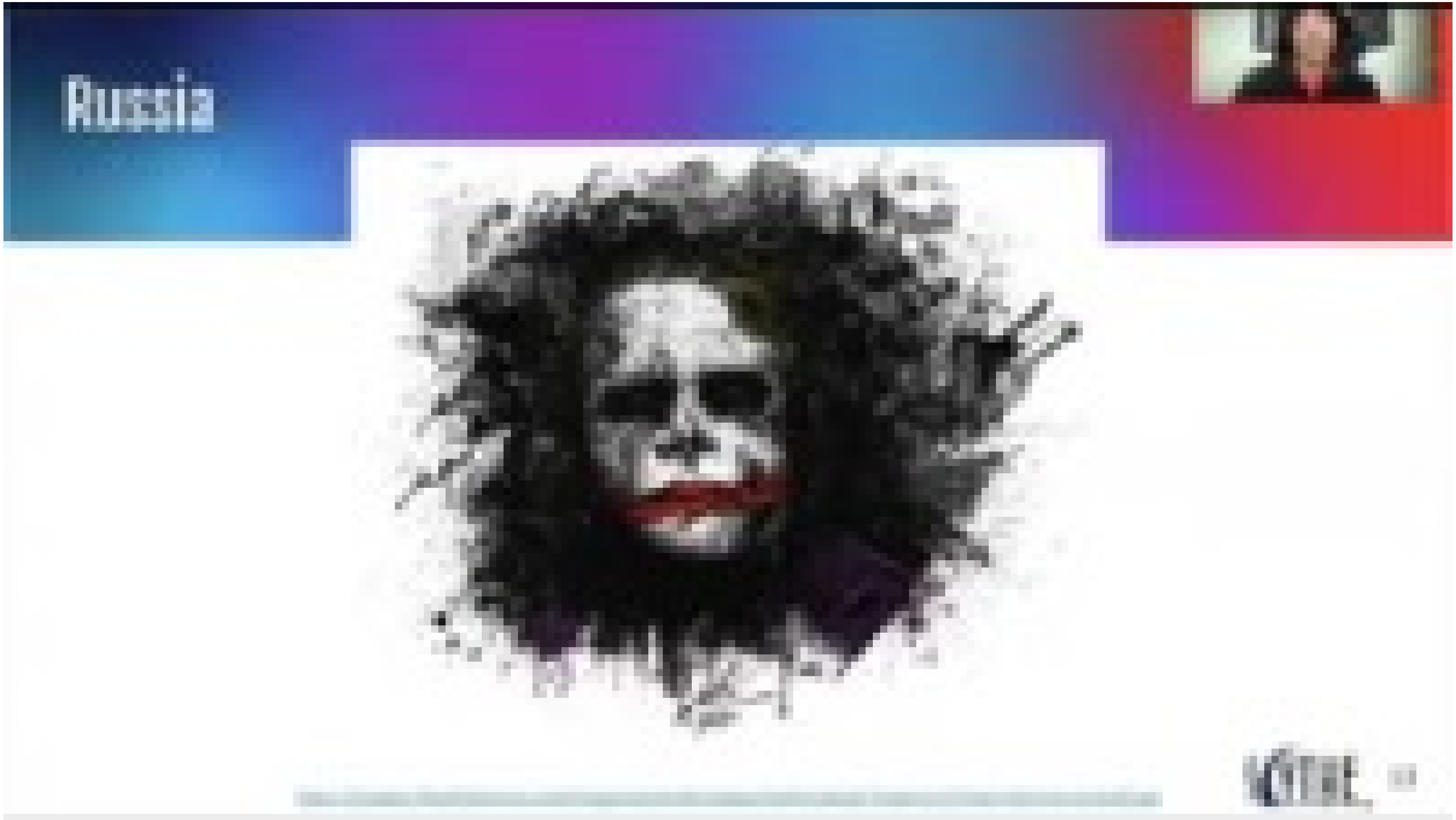
LTC Erica Mitchell,

Army Cyber Institute

Keynote Session with Bryson Bort

Bryson is the Founder of SCYTHE, a start-up building a next generation attack emulation platform, and GRIMM, a cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system security. He is a Senior Fellow for Cybersecurity and National Security at R Street and the National Security Institute and an Advisor to the Army Cyber Institute. As a U.S. Army Officer, he served as a Battle Captain and Brigade Engineering Officer in support of Operation Iraqi Freedom before leaving the Army as a Captain. He was recognized as one of the Top 50 in Cyber in 2020 by Business Insider.

Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point. He holds a Master's Degree in Telecommunications Management from the University of Maryland, a Master's in Business Administration from the University of Florida, and completed graduate studies in Electrical Engineering and Computer Science at the University of Texas.



Russia

Questions?

Break

JACK VOLTAIC

conference series

Prepare | Prevent | Respond | Report

June 23, 2021

Technology Integration and Cyber Resilience

NUARI 1819 Norwich University Applied Research Institutes

The Citadel

Army Cyber Institute at West Point

Georgia Cyber Center Augusta University

University of Illinois Urbana-Champaign

Welcome to the Conference

9:00 – 9:15 am	Welcome & Introduction	Phil Sussman (President, NUARI)
9:15 – 9:30 am	Jack Voltaic 3.0 Background and NUARI Role	LTC Erica Mitchell (ACI)
9:30 – 10:10 am	Critical Infrastructure and Cyber Resilience	Bryson Bort (Scythe)
10:10 – 10:20 am	Break	
10:20 – 11:00 am	Using Analytic Tools to Identify Critical Infrastructure Dependencies using AHA	Tom Muehleisen (NUARI) Ryan Hruska (INL) MAJ Steve Whitham (ACI)
11:00 – 11:45 am	Challenges of Distributed Critical Infrastructure Exercises – Lessons Learned	Tom Muehleisen (NUARI) Joe Minicucci (NUARI) MAJ Steve Whitham (ACI)
11:45 am – 12:30 pm	Lunch break	
12:30 – 2:00 pm	ACI Technical Integration Project Background and Development Process	MAJ Steve Whitham (ACI) Mike Schulz (NUARI) TR Staake (NUARI) Evan Owen (52inc)
2:00 – 2:10 pm	Break	
2:10 – 3:30 pm	Technical Integration Proof of Concept Demo & Mini Exercise	Mike Schulz (NUARI) TR Staake (NUARI) MAJ Steve Whitham (ACI)
3:30 – 3:50 pm	Questions, Discussion, and Feedback	Kristen Pedersen (NUARI)
3:50 - 3:55 pm	Next Conference: Georgia Cyber Center - **Developing a Unified Approach to Critical Infrastructure**	Eric Toler (GCC) MAJ Steve Whitham (ACI)
3:55 - 4:00 pm	Closing	Kristen Pedersen (NUARI)

Using Analytic Tools and AHA to Identify Critical Infrastructure Dependencies

Tom Muehleisen, NUARI

Ryan Hruska, Idaho National Lab

Jun 23, 2021

Ryan Hruska

Chief Scientist – Infrastructure Analysis

INL Mission Assurance

Jack Voltaic Conference Series: Technology Integration for Cyber Resilience

NUARI
Norwich University Applied Research Institutes

decide® PLATFORM

INL Idaho National Laboratory

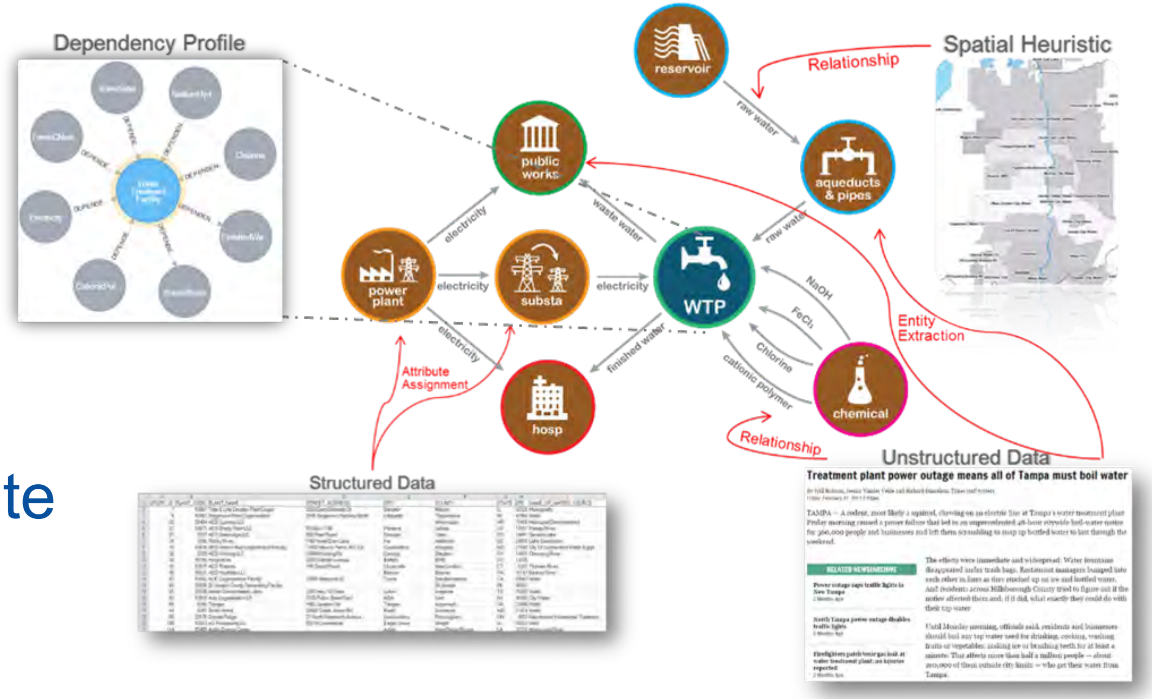
INL Mission & Dependency Analysis

- Provide actionable information – Get the right information to the right person, at the right time.
  - Enhance the **continuity of operations** across sectors and organizations
  - Understand the impact/consequence of infrastructure failure
  - Enable collection and documentation of dependency information
  - Provide a framework and capability for both analysts & decision makers

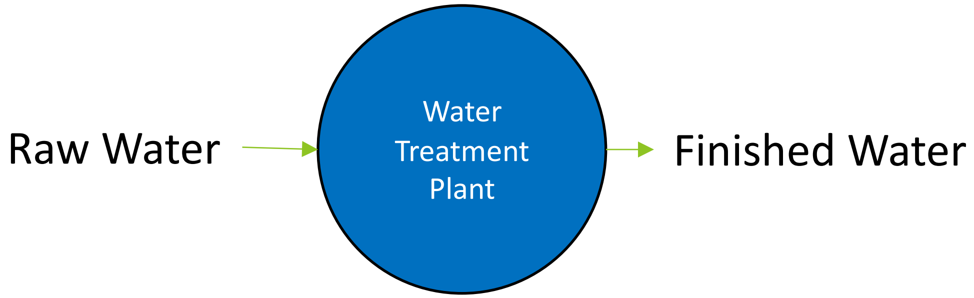
Prepare | Protect | Mitigate | Respond | Recover

All Hazards Analysis (AHA)

- Optimized framework for the collection, storage, analysis, and visualization of critical infrastructure information.
- Provides ability to store and model infrastructure systems as linked multigraphs providing an intuitive and natural representation.
- Provides the foundation to rapidly evaluate and understand the potential consequences of manmade and natural disaster on infrastructure systems.



Generic Dependency Profile

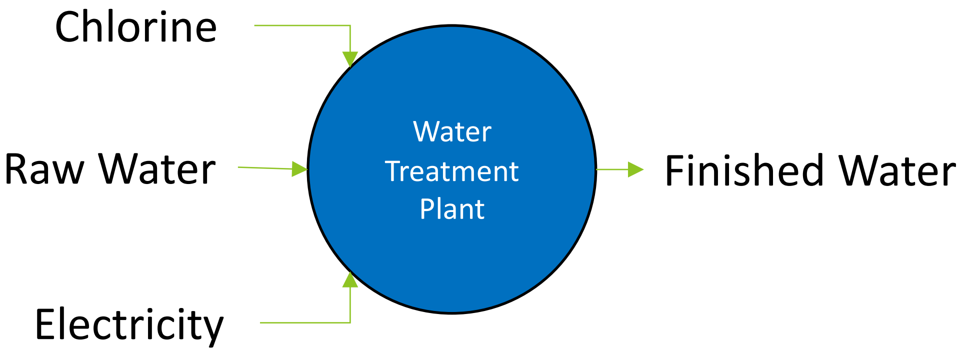


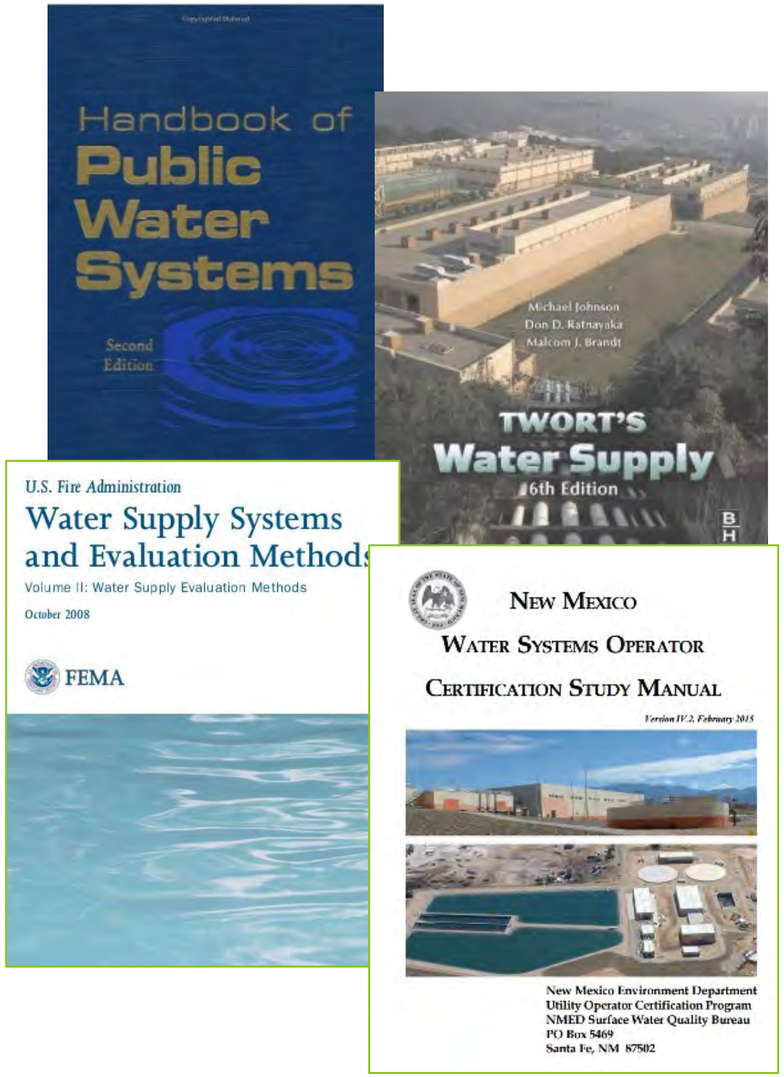
Raw Water

Water Treatment Plant

Finished Water

Generic Dependency Profile




Handbook of Public Water Systems

Second Edition

Michael Johnson
Don D. Ratnayaka
Malcom J. Brandt

TWORT'S Water Supply

6th Edition

U.S. Fire Administration

Water Supply Systems and Evaluation Method

Volume II: Water Supply Evaluation Methods

October 2008

FEMA

NEW MEXICO

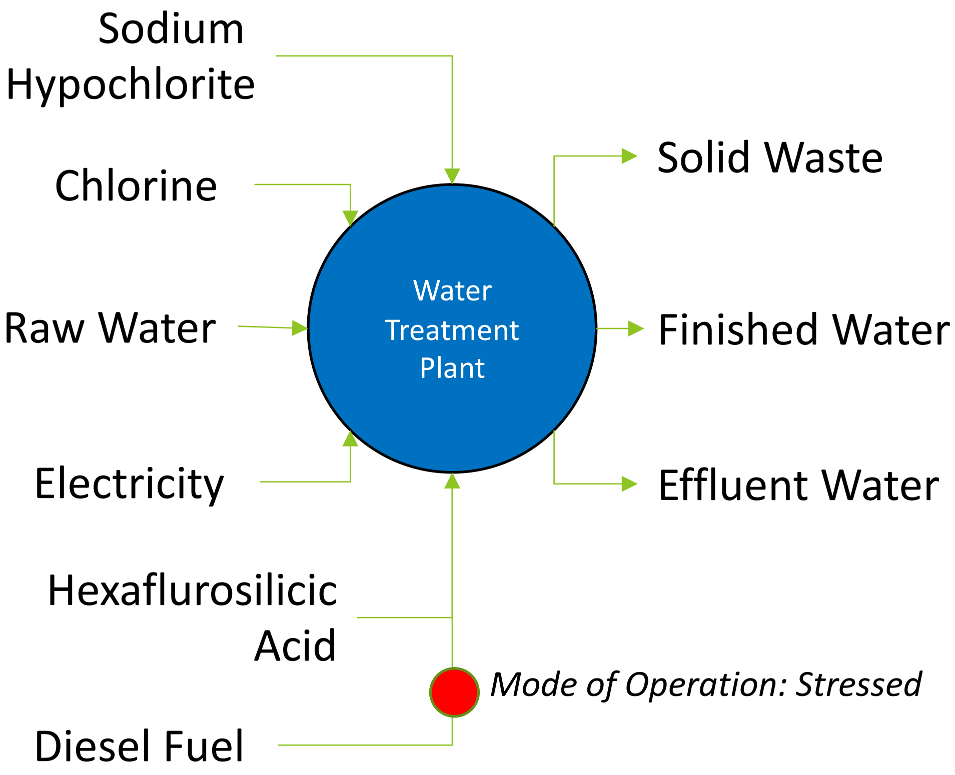
WATER SYSTEMS OPERATOR

CERTIFICATION STUDY MANUAL

Version IV.2, February 2015

New Mexico Environment Department
Utility Operator Certification Program
NMED Surface Water Quality Bureau
PO Box 5469
Santa Fe, NM 87502

Generic Dependency Profile



Sodium Hypochlorite

Chlorine

Raw Water

Electricity

Hexaflurosilicic Acid

Diesel Fuel

Water Treatment Plant

Solid Waste

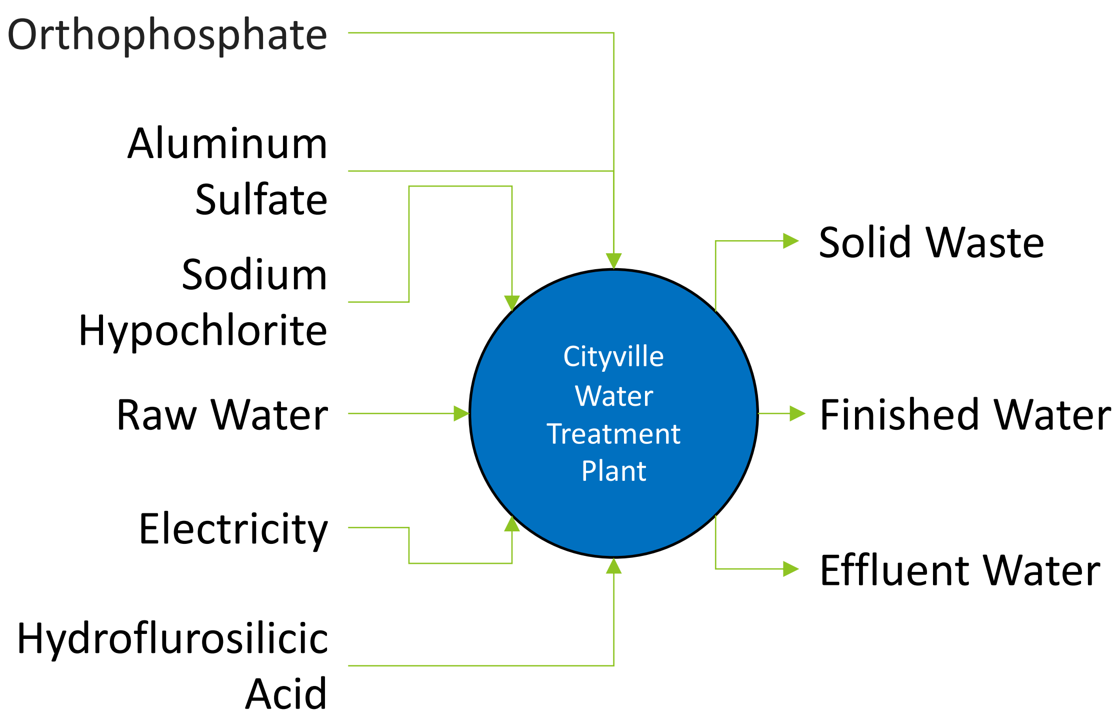
Finished Water

Effluent Water

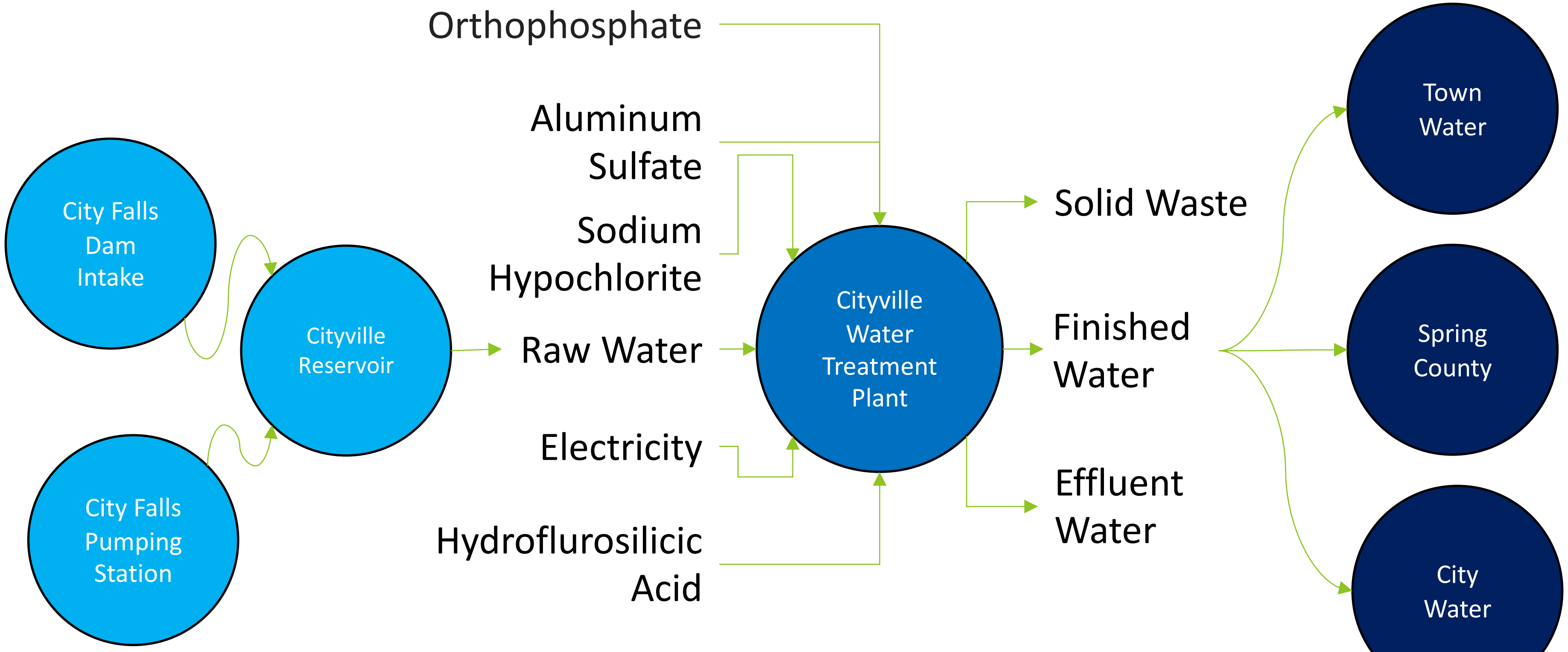
Mode of Operation: Stressed

Previous Assessments

Facility Specific Dependency Profile



Regional Dependency Models



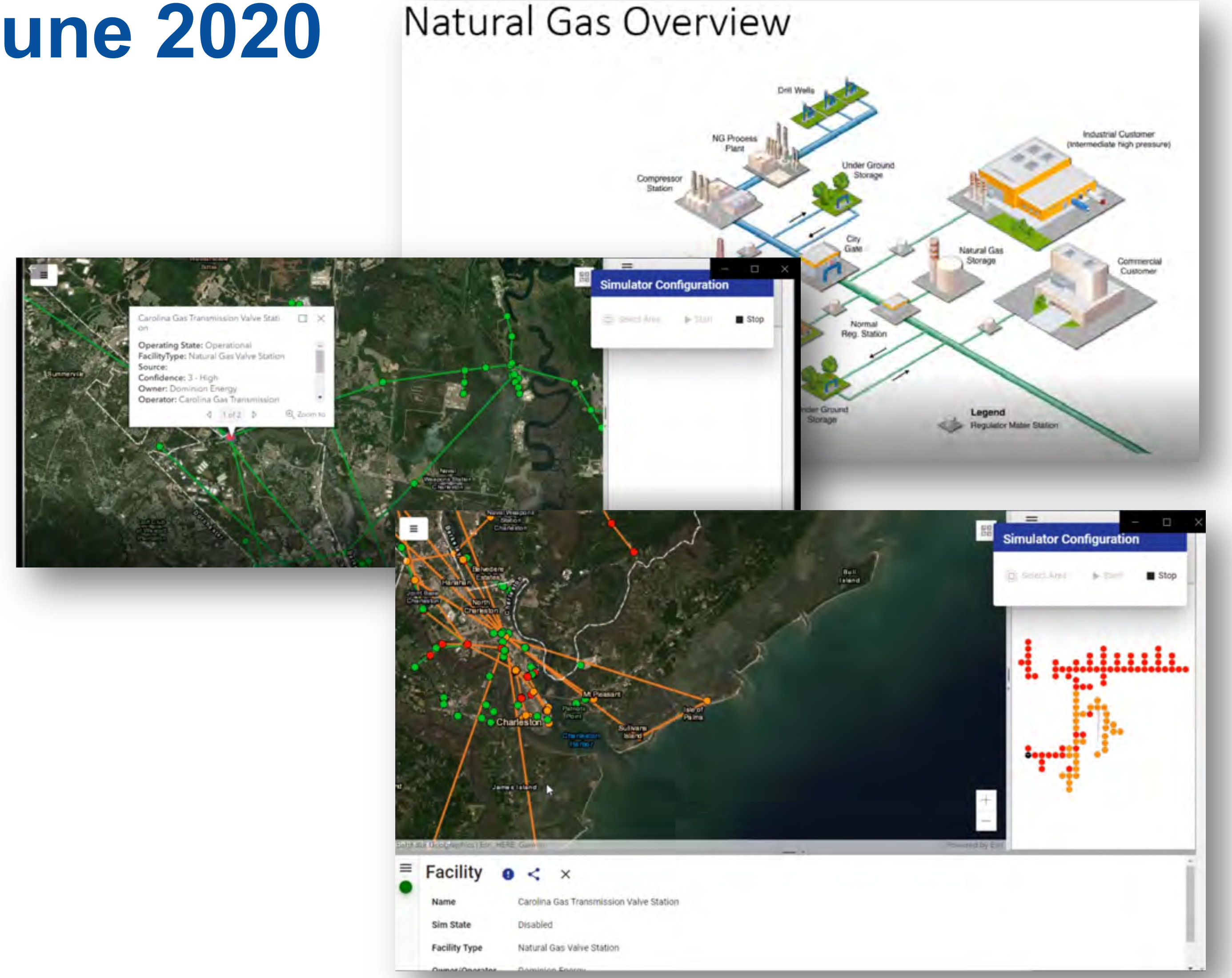
Jack Pandemus (JV3)
Mini-Exercise 9 & 16 June 2020

Purpose

Jack Pandemus is distributed functional exercise and part of Jack Voltaic 3 (JV3). This semi-generic scenario, presented on the DECIDE® platform and using web-conferencing (TBD), explores a gas pipeline disruption, caused by a cyber attack, which in turn, causes issues with electrical power generation and healthcare. All of these events occur during an ongoing Pandemic Response.

Goals

1. Maintain engagement with the JV3 stakeholder organizations in Charleston and Savannah.
2. Encourage the use of analytic tools (e.g. INL's AHA) to support better understanding of Community Lifelines and Critical Functions.
3. Capture lessons learned from the current crisis (pandemic).

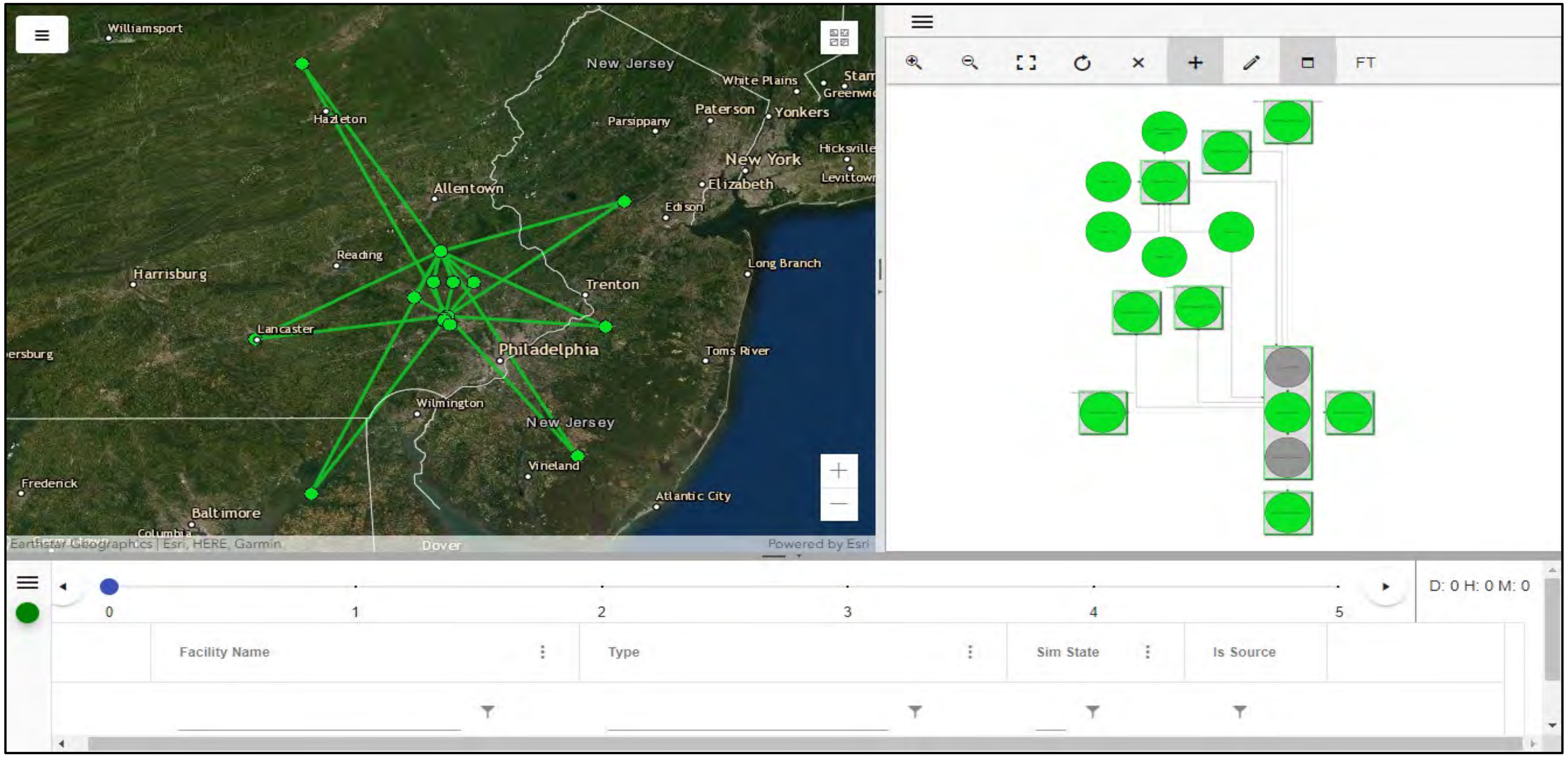


Carolina Gas Transmission Valve Station

Operating State: Operational
FacilityType: Natural Gas Valve Station
Source:
Confidence: 3 - High
Owner: Dominion Energy
Operator: Carolina Gas Transmission

Name: Carolina Gas Transmission Valve Station
Sim State: Disabled
Facility Type: Natural Gas Valve Station
Owner/Operator: Dominion Energy

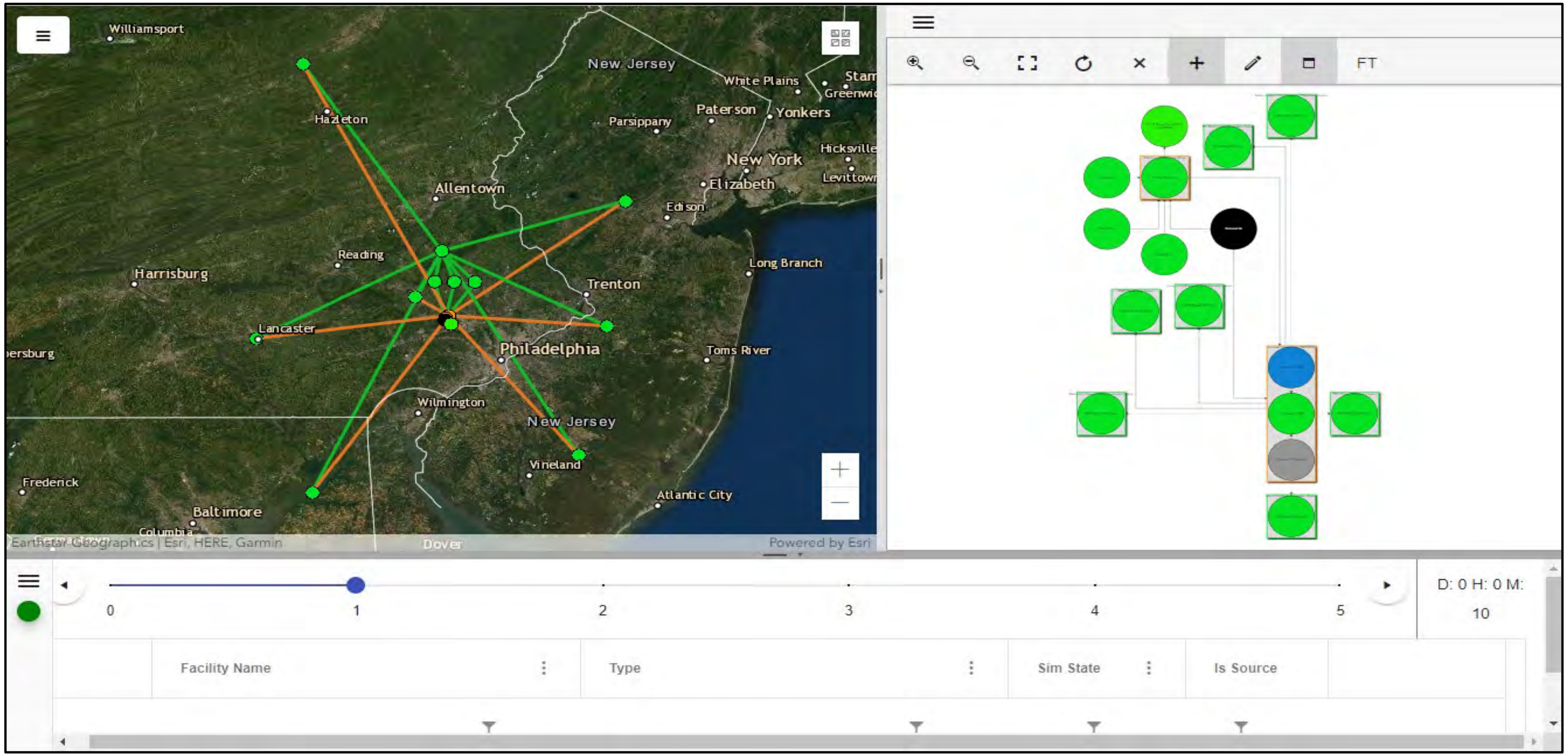
Impact Analysis – Event Capability- Normal Operations



D: 0 H: 0 M: 0

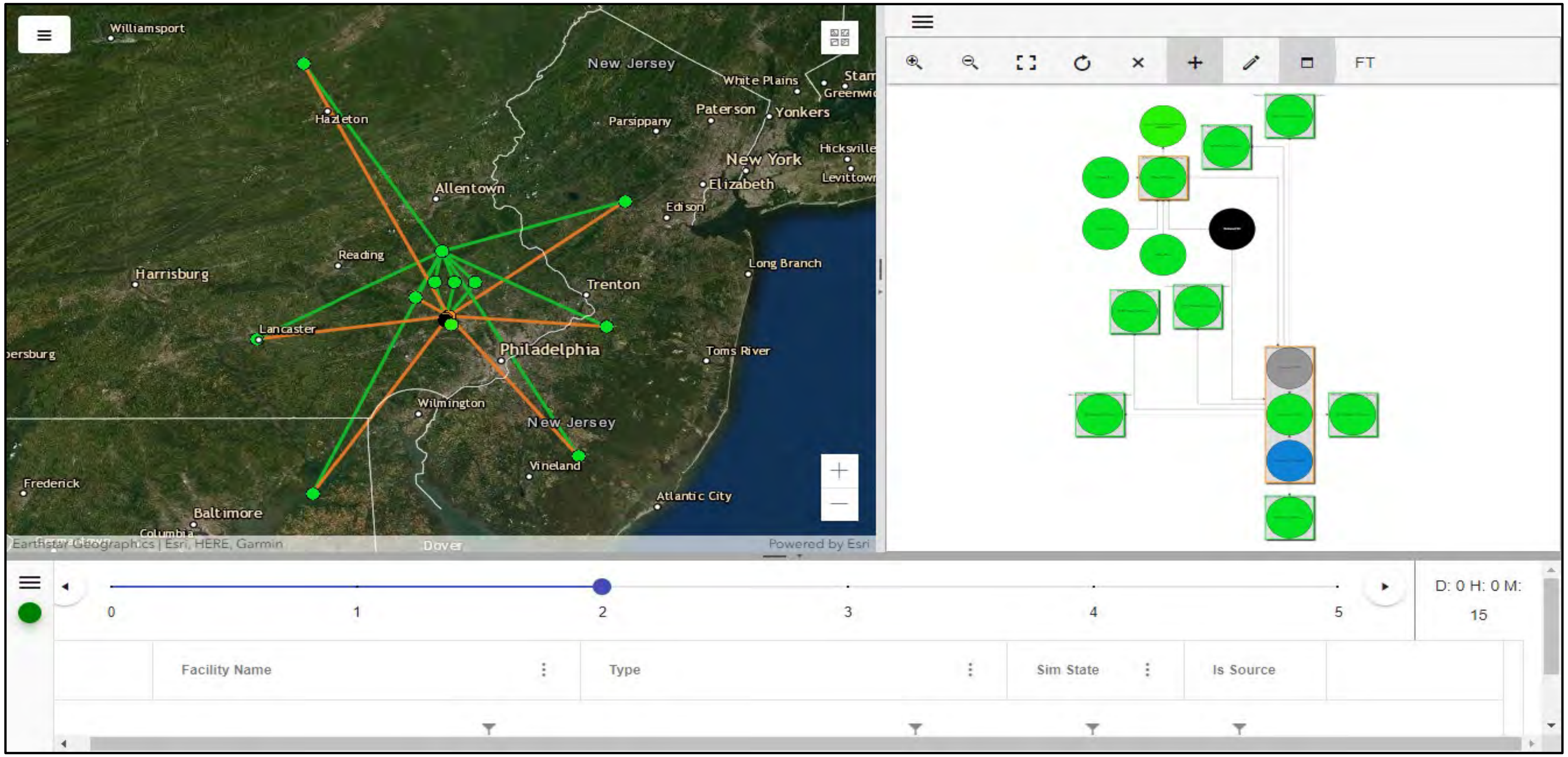
Facility Name	Type	Sim State	Is Source

Impact Analysis – Event Capability- Substation Outage - UPS



Facility Name	Type	Sim State	Is Source

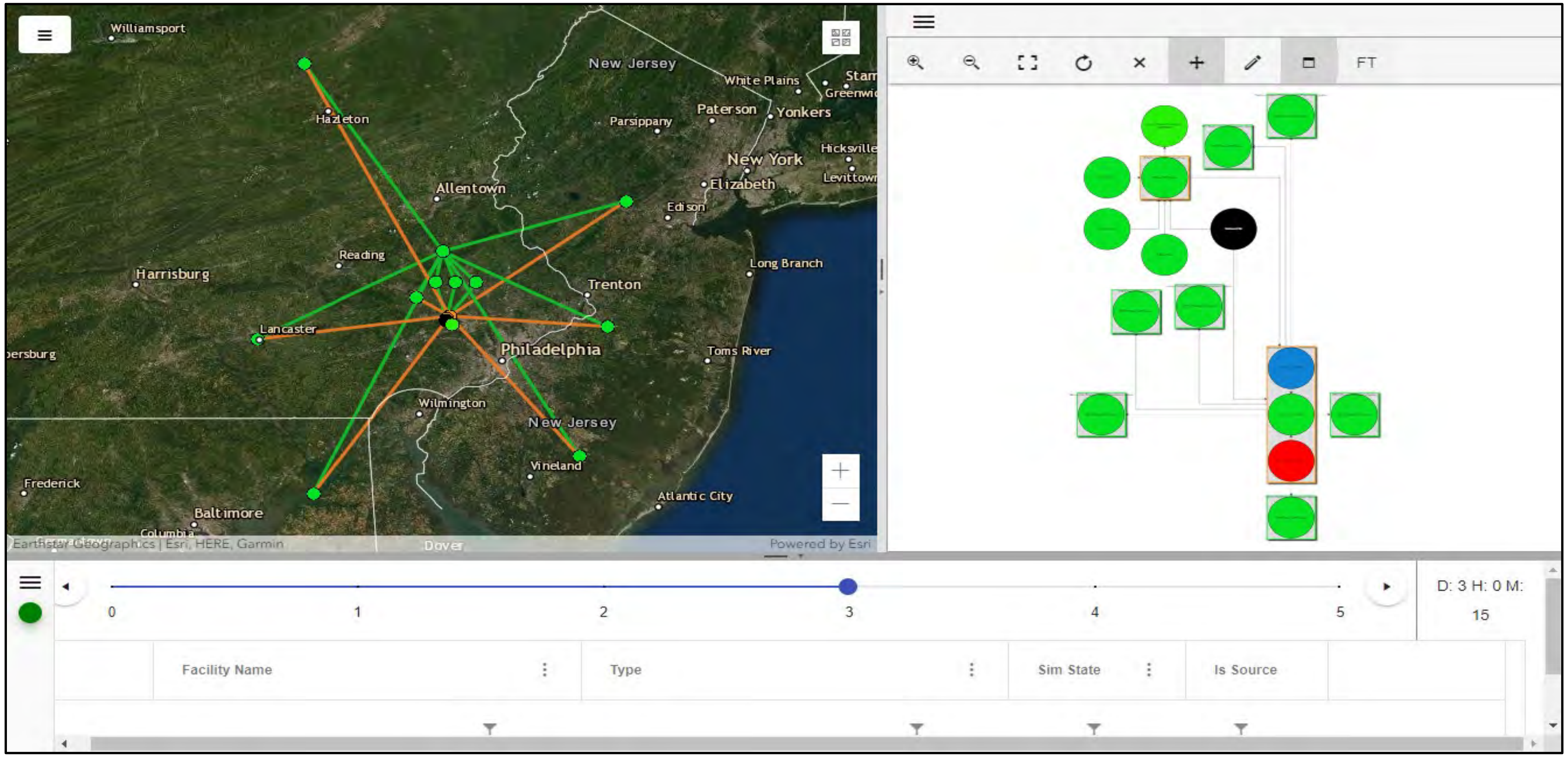
Impact Analysis – Event Capability- Back-Up Generation



D: 0 H: 0 M: 15

Facility Name	Type	Sim State	Is Source

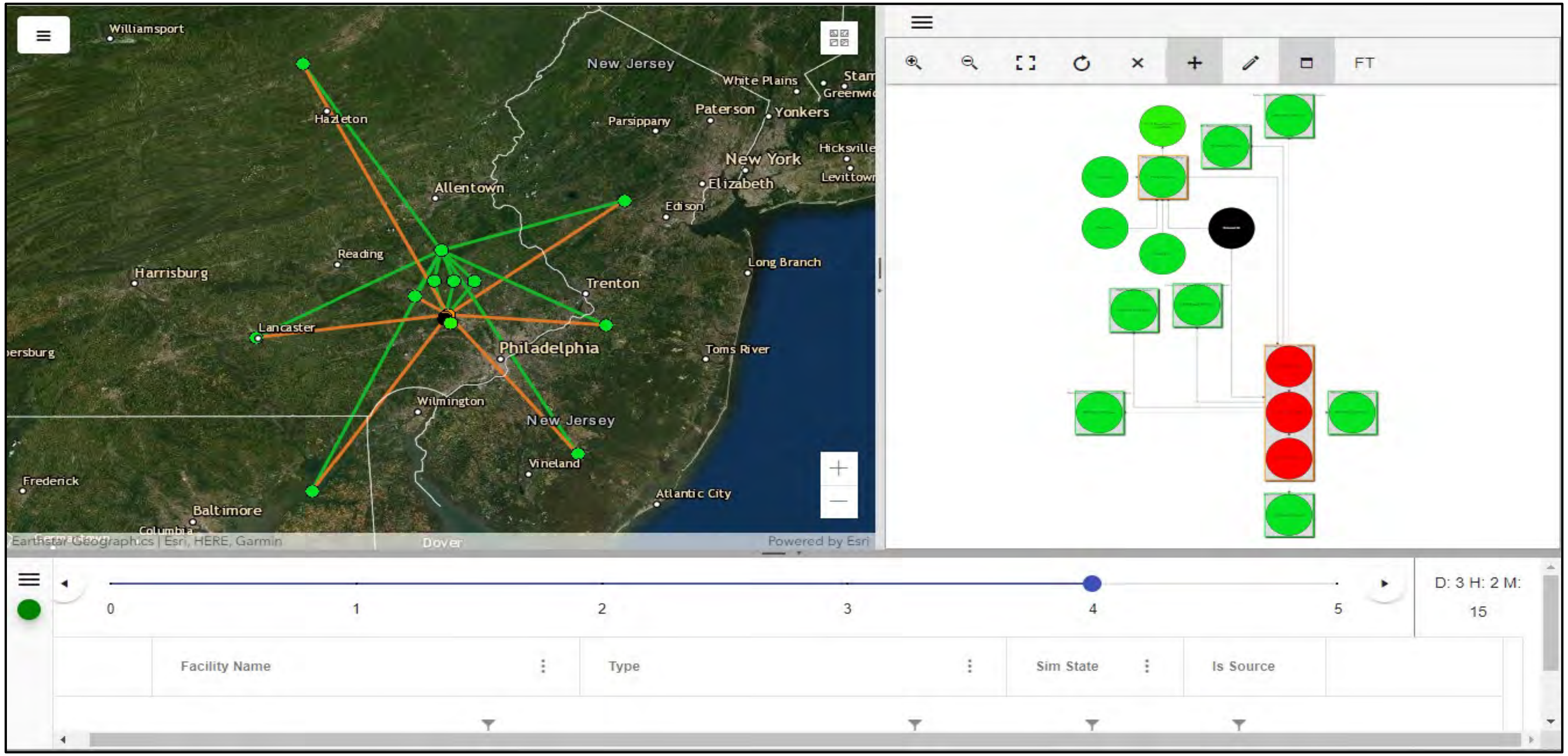
Impact Analysis – Event Capability- UPS



D: 3 H: 0 M: 15

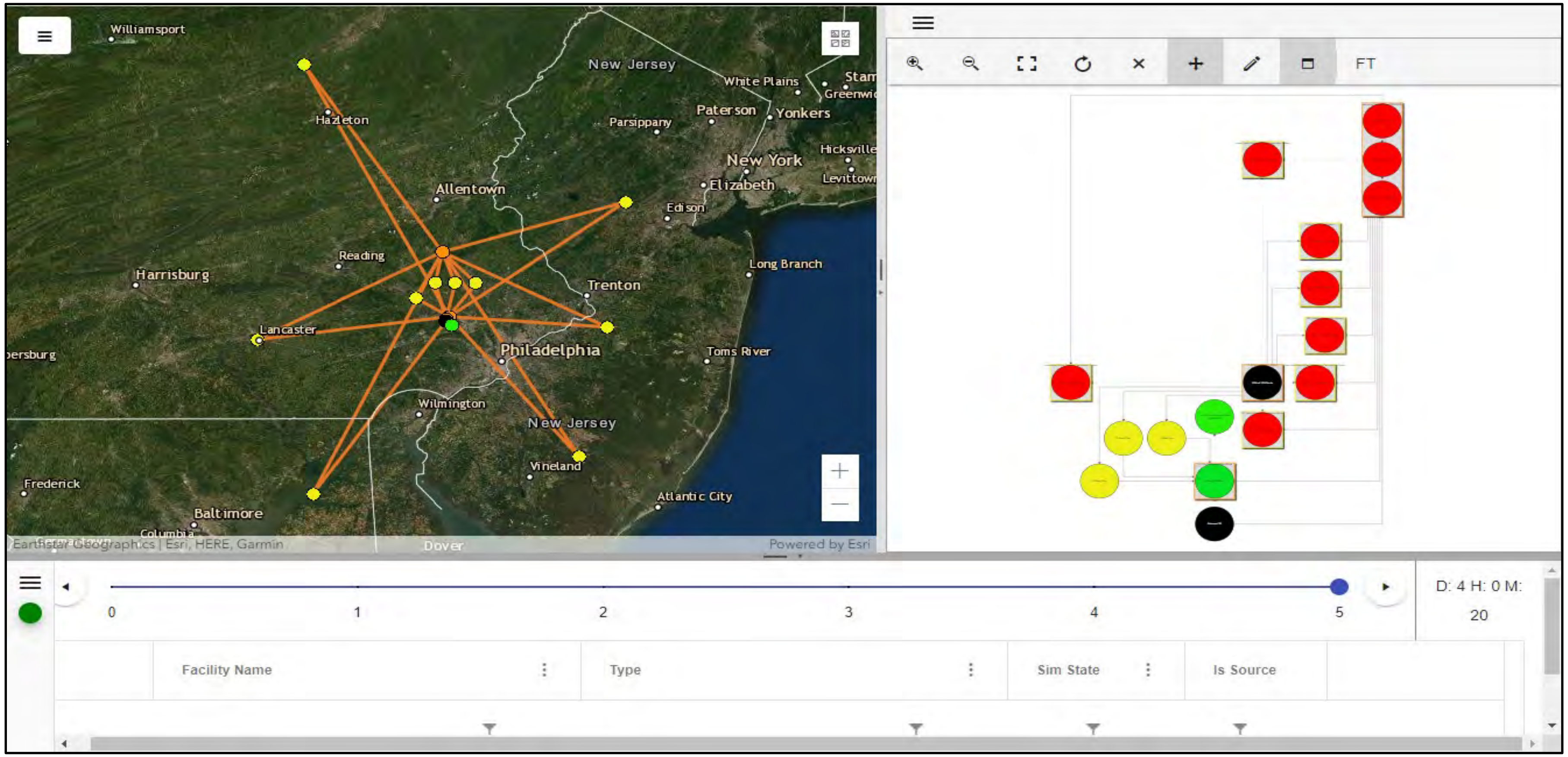
Facility Name	Type	Sim State	Is Source

Impact Analysis – Event Capability- Redundant Central Office



Facility Name	Type	Sim State	Is Source

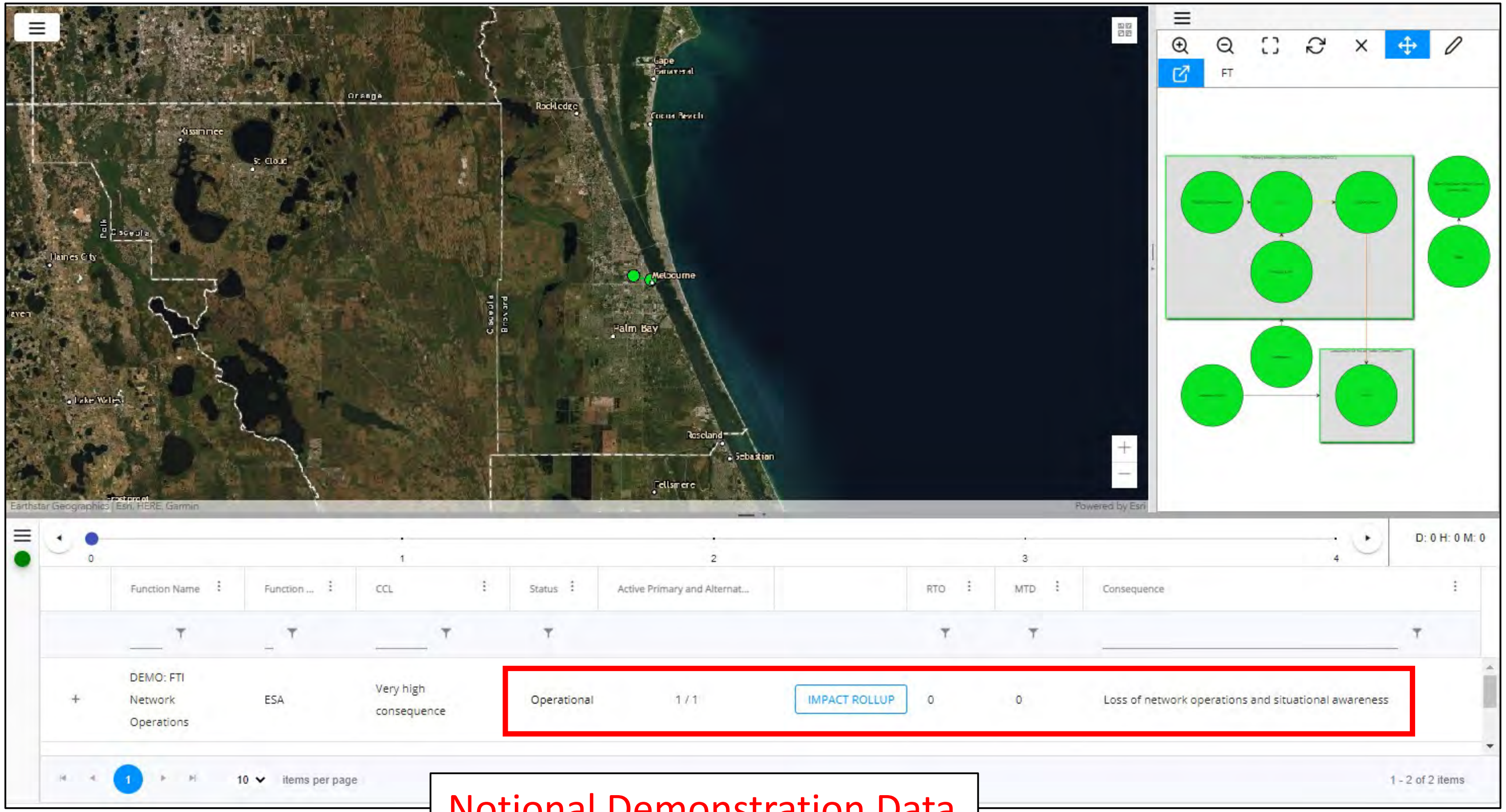
Impact Analysis – Event Capability- Network Router



D: 4 H: 0 M: 20

Facility Name	Type	Sim State	Is Source

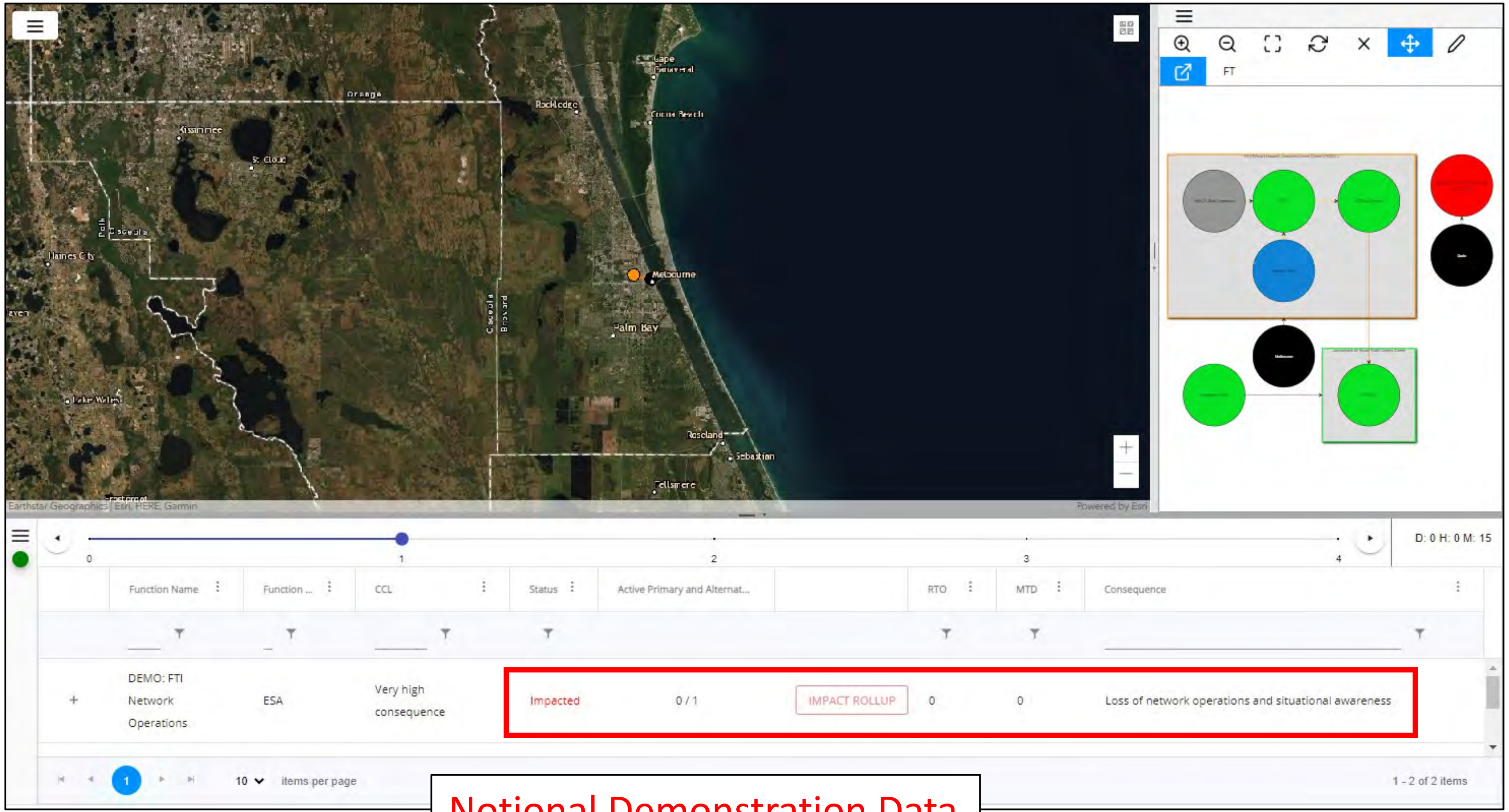
Essential Function Analysis Capability (EFAC) - Simulation – Normal Operations



	Function Name	Function ...	CCL	Status	Active Primary and Alternat...		RTO	MTD	Consequence
+	DEMO: FTI Network Operations	ESA	Very high consequence	Operational	1 / 1	IMPACT ROLLUP	0	0	Loss of network operations and situational awareness

Notional Demonstration Data

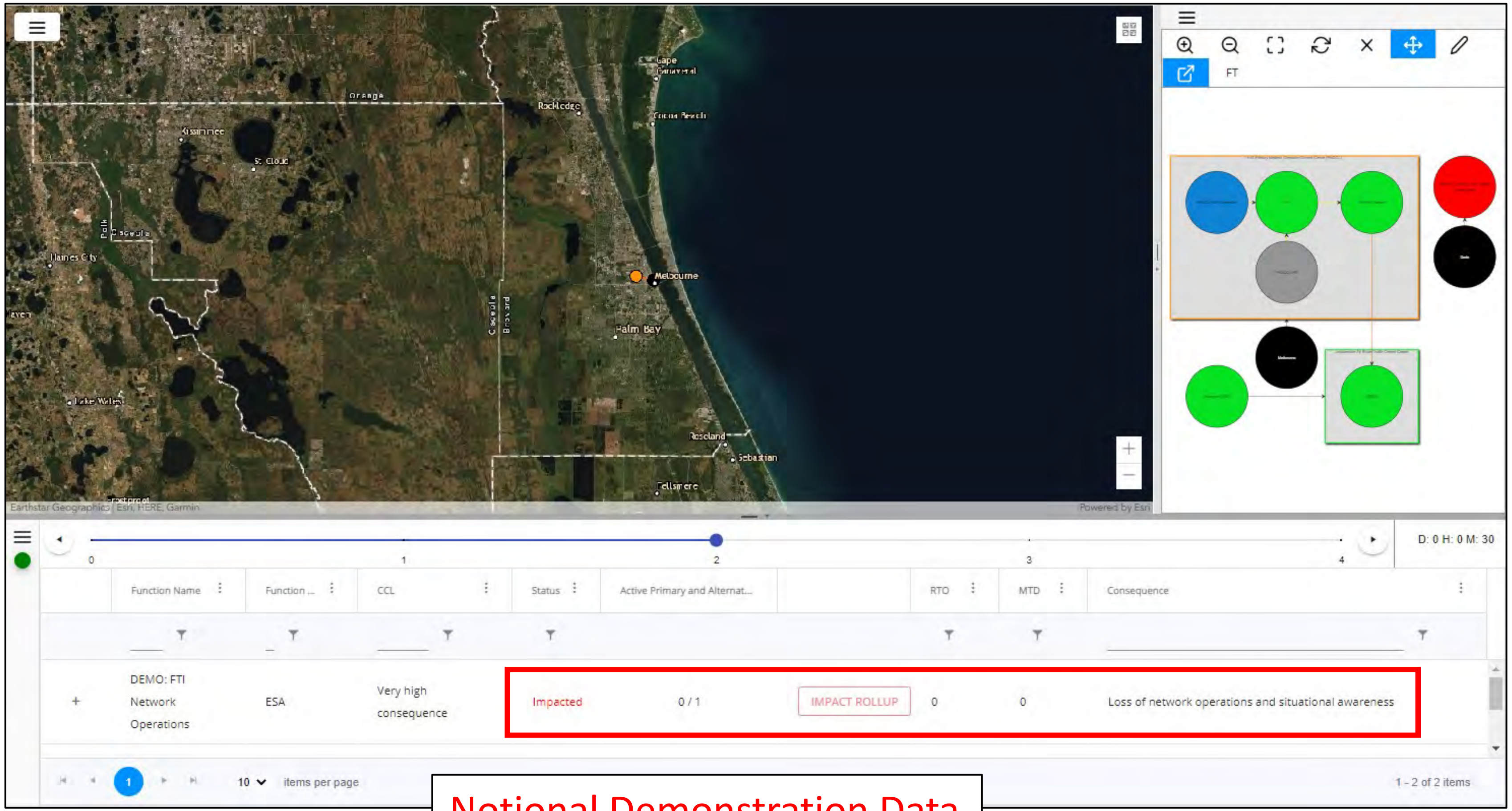
Essential Function Analysis Capability (EFAC) - Simulation – Substation Failure



Function Name	Function ...	CCL	Status	Active Primary and Alternat...		RTO	MTD	Consequence
DEMO: FTI Network Operations	ESA	Very high consequence	Impacted	0 / 1	IMPACT ROLLUP	0	0	Loss of network operations and situational awareness

Notional Demonstration Data

Essential Function Analysis Capability (EFAC) - Simulation – Back-Up Generation

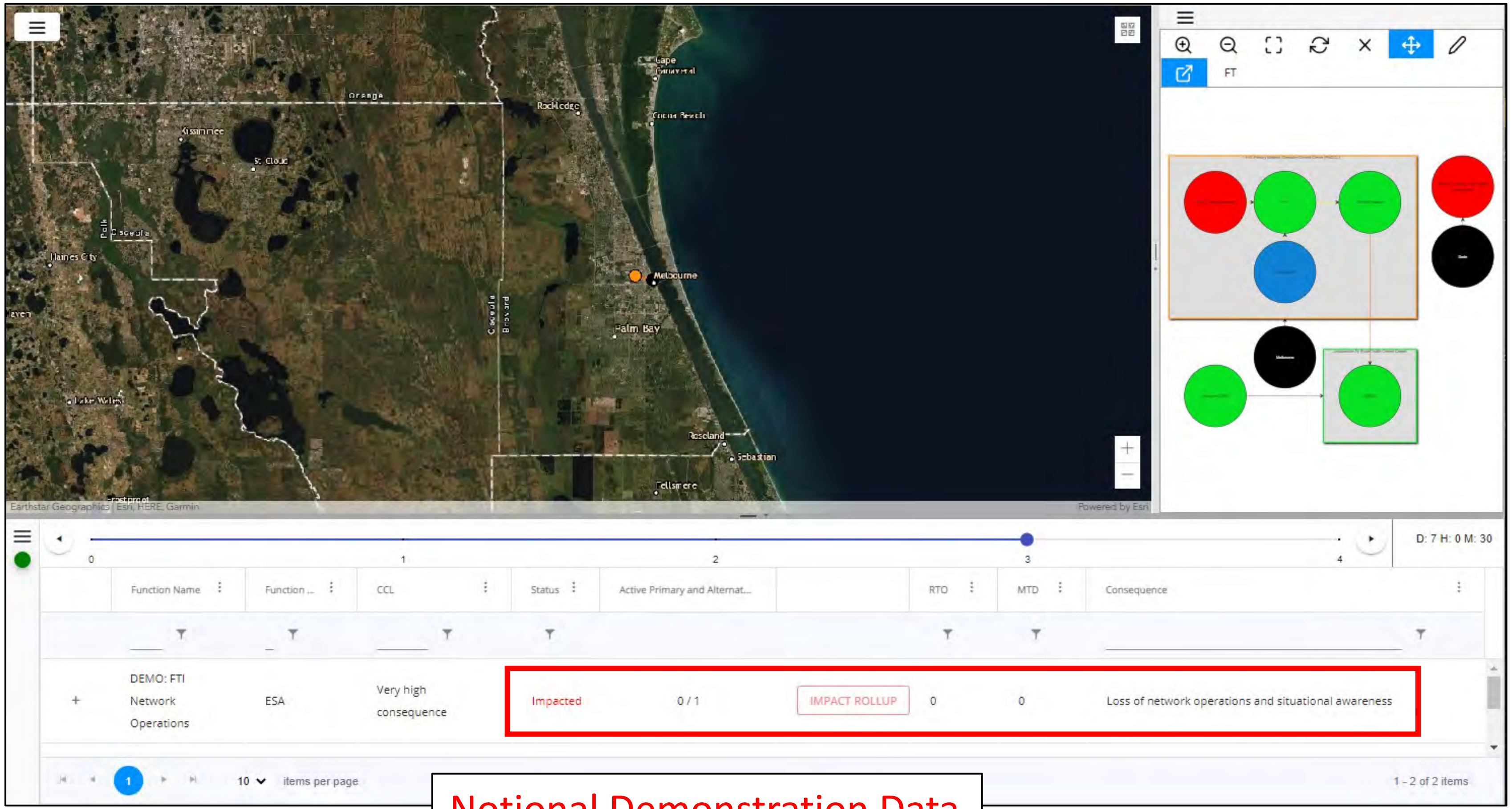


	Function Name	Function ...	CCL	Status	Active Primary and Alternat...		RTO	MTD	Consequence
+	DEMO: FTI Network Operations	ESA	Very high consequence	Impacted	0 / 1	IMPACT ROLLUP	0	0	Loss of network operations and situational awareness

1 10 items per page 1 - 2 of 2 items

Notional Demonstration Data

Essential Function Analysis Capability (EFAC) - Simulation - Generator: Loss of Fuel

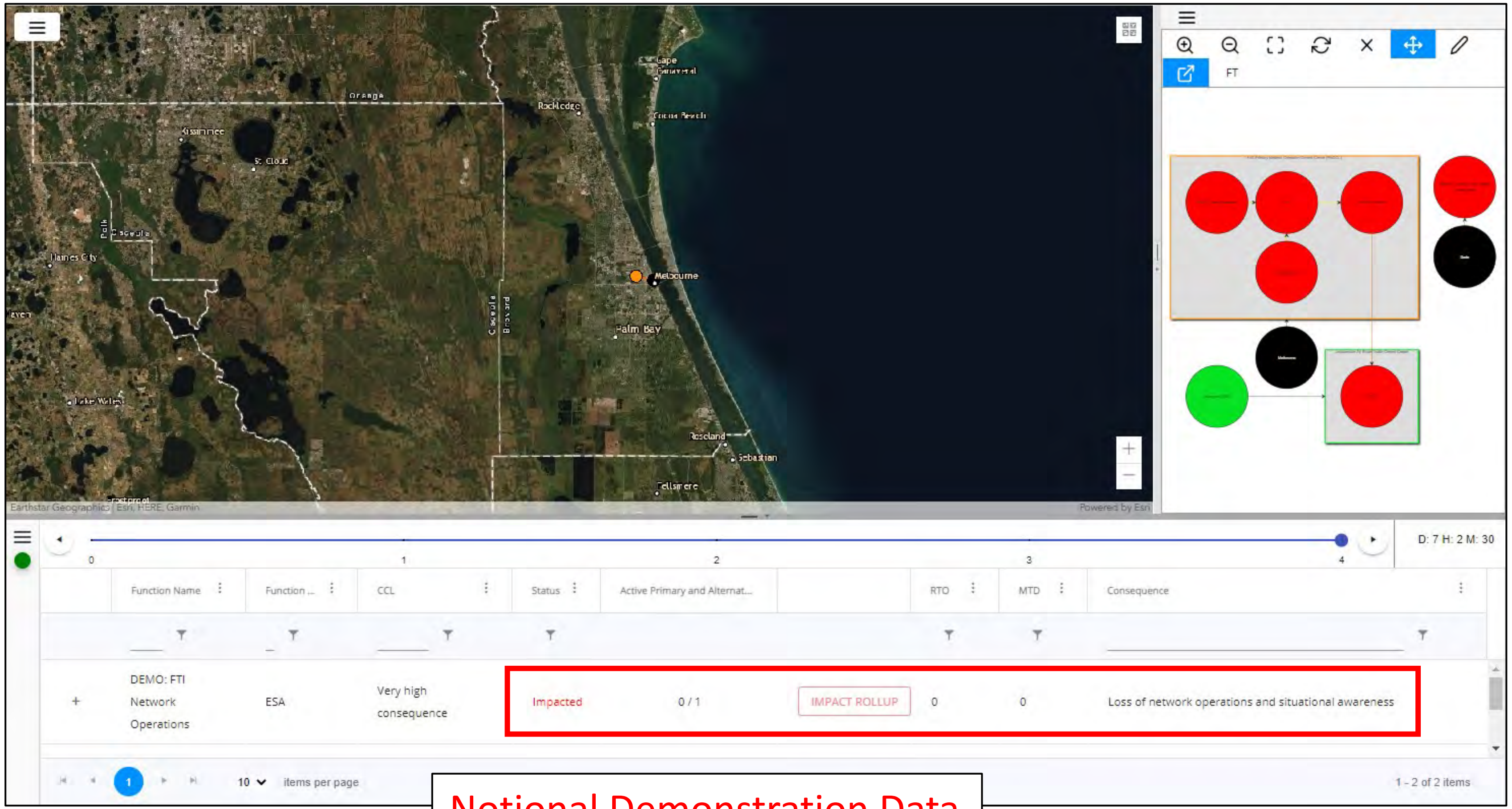


	Function Name	Function ...	CCL	Status	Active Primary and Alternat...		RTO	MTD	Consequence
+	DEMO: FTI Network Operations	ESA	Very high consequence	Impacted	0 / 1	IMPACT ROLLUP	0	0	Loss of network operations and situational awareness

1 10 items per page 1 - 2 of 2 items

Notional Demonstration Data

Essential Function Analysis Capability (EFAC) - Simulation – Loss of Power



D: 7 H: 2 M: 30

	Function Name	Function ...	CCL	Status	Active Primary and Alternat...		RTO	MTD	Consequence
+	DEMO: FTI Network Operations	ESA	Very high consequence	Impacted	0 / 1	IMPACT ROLLUP	0	0	Loss of network operations and situational awareness

10 items per page

1 - 2 of 2 items

Notional Demonstration Data

Wrap-Up & Action Items

- Is a dynamic knowledge framework that provides
  - Scale Independent Functional Decomposition for Continuity of Operations Planning and Analysis
    - Essential Function Analysis
      - Simulation (Contingency Analysis)
        - All Hazards
  - Adaptable Methodology
  - Knowledge Transfer & Knowledge Management
  - Decision Support

Contact Information:
Ryan.Hruska@inl.gov

Questions?

Tom Muehleisen, NUARI

Joe Minicucci, NUARI

Challenges of Distributed Critical Infrastructure Exercises – Lessons Learned during Jack Voltaic 3.0

Spanning Critical Functions and Incorporating Key Community Lifelines using a Middle-Down Approach

Background: JV3 ACI Report

- JV3 examined impact of a cyber event on Army Force Projection
- Reinforced a Whole-of-Community approach
- Examined DSCA Cyber request/coord
- Continued the JV series intent of adaptable and repeatable

- For more information, please read the full report located on ACI's website:
  - https://cyber.army.mil/
  - Or click HERE for the report.

JACK VOLTAIC 3.0

Cyber Research Report

Prepare | Prevent | Respond

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.

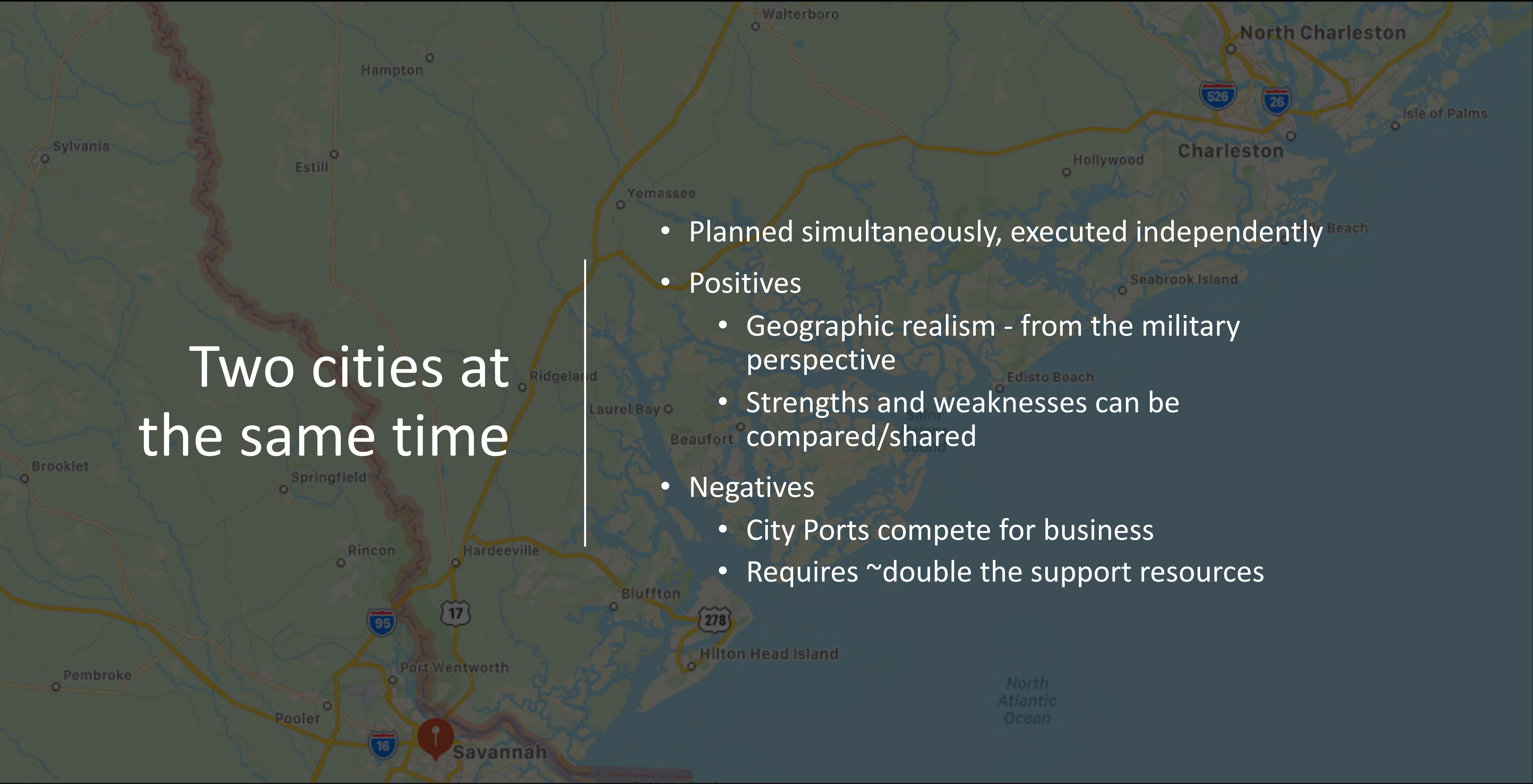
Lt. Col. Doug Fletcher | Lt. Col. Erica Mitchell | Maj. Erik Korn
Maj. Steve Whitham | Maj. Jason Hillman | Ron Yearwood
Clint Walker | Dr. Aryn Pyke | Dr. Gabriel Weaver | Brandon Pugh
Katherine Hutton | George Platsis | Timothy Klett | Ryan Hruska

ARMY CYBER INSTITUTE AT WEST POINT

FTI CONSULTING

Challenges and Solutions

- Two cities at same time
- Cultural differences and Process differences
- Critical Functions / Community Lifelines
- Distributed Exercise
- Tactical Stakeholders
- Cyber response mixed

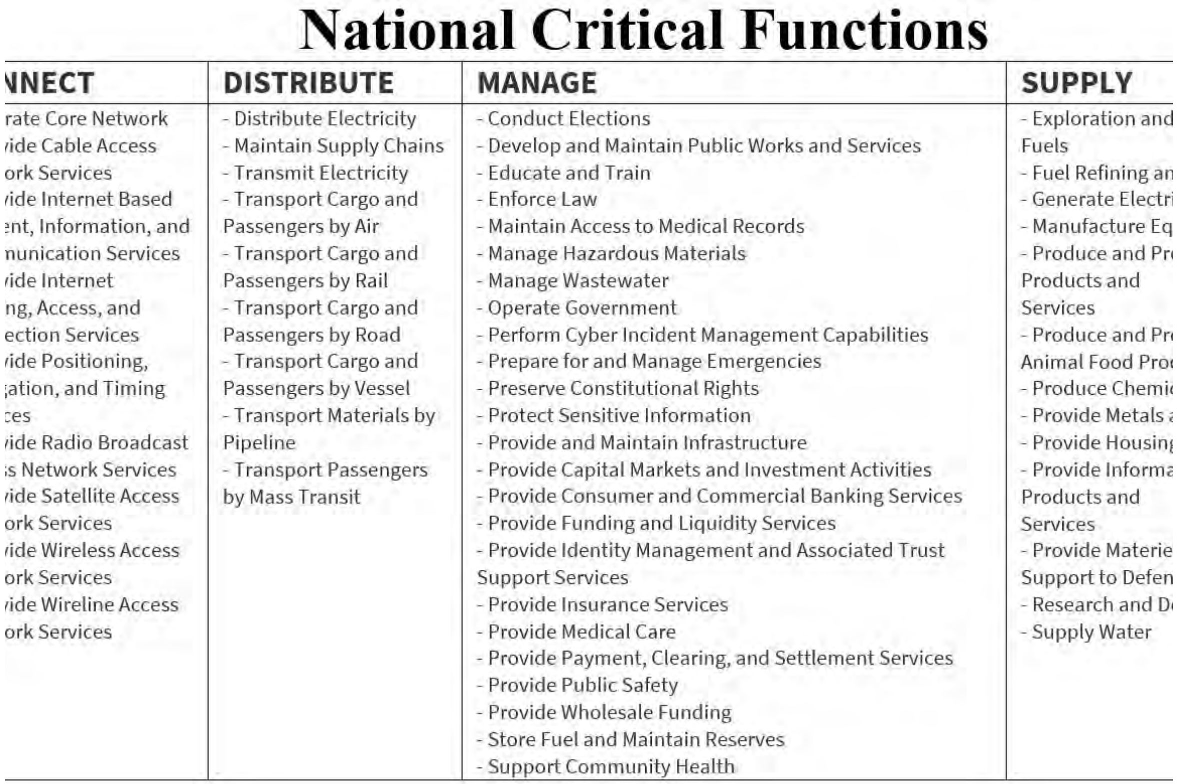


Two cities at the same time

- Planned simultaneously, executed independently
- Positives
  - Geographic realism - from the military perspective
  - Strengths and weaknesses can be compared/shared
- Negatives
  - City Ports compete for business
  - Requires ~double the support resources

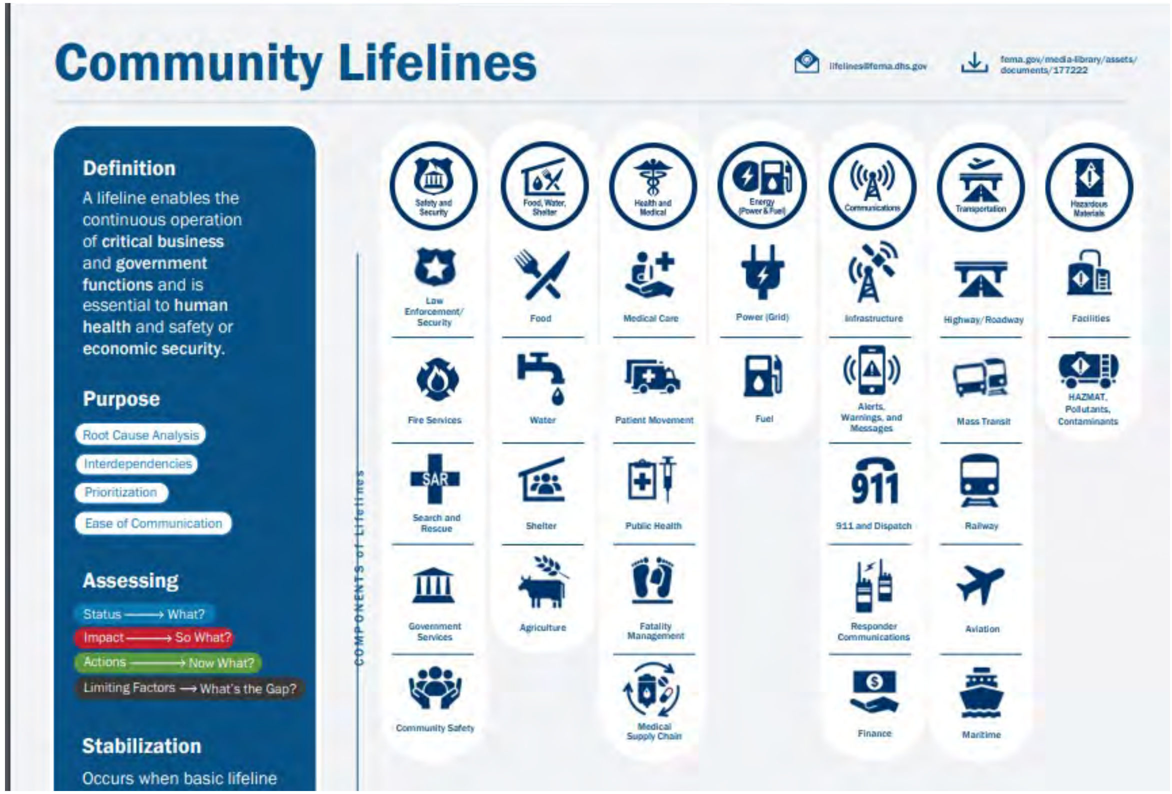
Cultural, Process and Political differences

- Military:
  - Differences between JELC and HSEEP
  - Academia (ACI) vs Operational (SDDC)
  - Data collection plan - kill the ant with a sledgehammer
- State/County
  - Weren't getting the same people from city or port - missing some things
  - County Directory of Emergency Mgmt - right level of engagement
- City
  - Level of engagement of organizations were different as well. City problem
  - Getting to transparency – tied to political – what can be said/not said; reveal/not reveal



National Critical Functions

NNECT	DISTRIBUTE	MANAGE	SUPPLY
rate Core Network ide Cable Access ork Services ide Internet Based ent, Information, and nunication Services ide Internet ng, Access, and ection Services ide Positioning, ation, and Timing ces ide Radio Broadcast s Network Services ide Satellite Access ork Services ide Wireless Access ork Services ide Wireline Access ork Services	- Distribute Electricity - Maintain Supply Chains - Transmit Electricity - Transport Cargo and Passengers by Air - Transport Cargo and Passengers by Rail - Transport Cargo and Passengers by Road - Transport Cargo and Passengers by Vessel - Transport Materials by Pipeline - Transport Passengers by Mass Transit	- Conduct Elections - Develop and Maintain Public Works and Services - Educate and Train - Enforce Law - Maintain Access to Medical Records - Manage Hazardous Materials - Manage Wastewater - Operate Government - Perform Cyber Incident Management Capabilities - Prepare for and Manage Emergencies - Preserve Constitutional Rights - Protect Sensitive Information - Provide and Maintain Infrastructure - Provide Capital Markets and Investment Activities - Provide Consumer and Commercial Banking Services - Provide Funding and Liquidity Services - Provide Identity Management and Associated Trust Support Services - Provide Insurance Services - Provide Medical Care - Provide Payment, Clearing, and Settlement Services - Provide Public Safety - Provide Wholesale Funding - Store Fuel and Maintain Reserves - Support Community Health	- Exploration and Fuels - Fuel Refining an - Generate Electri - Manufacture Eq - Produce and Pr Products and Services - Produce and Pr Animal Food Pro - Produce Chemi - Provide Metals - Provide Housin - Provide Informa Products and Services - Provide Materie Support to Defen - Research and D - Supply Water



Community Lifelines

lifelines@fema.dhs.gov

fema.gov/media-library/assets/documents/177222

Definition

A lifeline enables the continuous operation of **critical business** and government **functions** and is essential to human **health** and safety or **economic security.**

Purpose

- Root Cause Analysis
- Interdependencies
- Prioritization
- Ease of Communication

Assessing

- Status ——→ What?
- Impact ——→ So What?
- Actions ——→ Now What?
- Limiting Factors → What's the Gap?

Stabilization

Occurs when basic lifeline

COMPONENTS of Lifelines

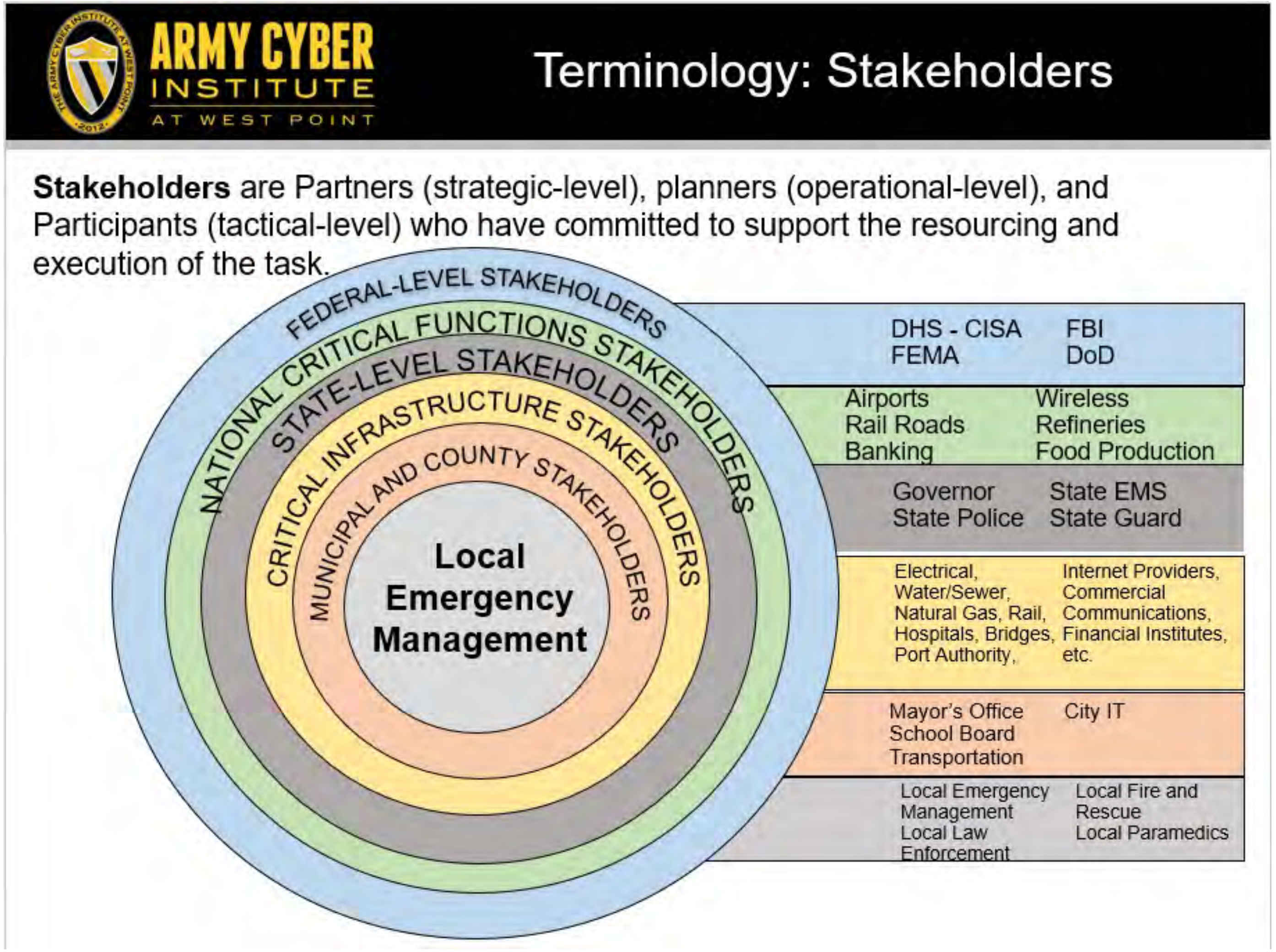
Safety and Security	Food, Water, Shelter	Health and Medical	Energy (Power & Fuel)	Communications	Transportation	Hazardous Materials
Law Enforcement/ Security	Food	Medical Care	Power (Grid)	Infrastructure	Highway/Roadway	Facilities
Fire Services	Water	Patient Movement	Fuel	Alerts, Warnings, and Messages	Mass Transit	HAZMAT, Pollutants, Contaminants
Search and Rescue	Shelter	Public Health		911 and Dispatch	Railway	
Government Services	Agriculture	Fatality Management		Responder Communications	Aviation	
Community Safety		Medical Supply Chain		Finance	Maritime	

Critical Functions / Community Lifelines

- Relationships between the stated national structures and the community structures
- City level objectives were generated from this
- Challenge was when hit lifeline level lost the fidelity (not right people in room…always hard but very important)

Tactical Stakeholders

- Did not get full city/county elected officials buy in (Top Down)
  - Engaged planning at the mid-level management (Middle Out)
- Approval from leaders to spend resources (people)
  - But no guidance and direction
- Strategic, Operational, Tactical
  - We targeted Operational/Tactical



ARMY CYBER INSTITUTE AT WEST POINT

Terminology: Stakeholders

Stakeholders are Partners (strategic-level), planners (operational-level), and Participants (tactical-level) who have committed to support the resourcing and execution of the task.

FEDERAL-LEVEL STAKEHOLDERS
NATIONAL CRITICAL FUNCTIONS STAKEHOLDERS
STATE-LEVEL STAKEHOLDERS
CRITICAL INFRASTRUCTURE STAKEHOLDERS
MUNICIPAL AND COUNTY STAKEHOLDERS
Local Emergency Management

DHS - CISA, FEMA, FBI, DoD

Airports, Rail Roads, Banking, Wireless, Refineries, Food Production

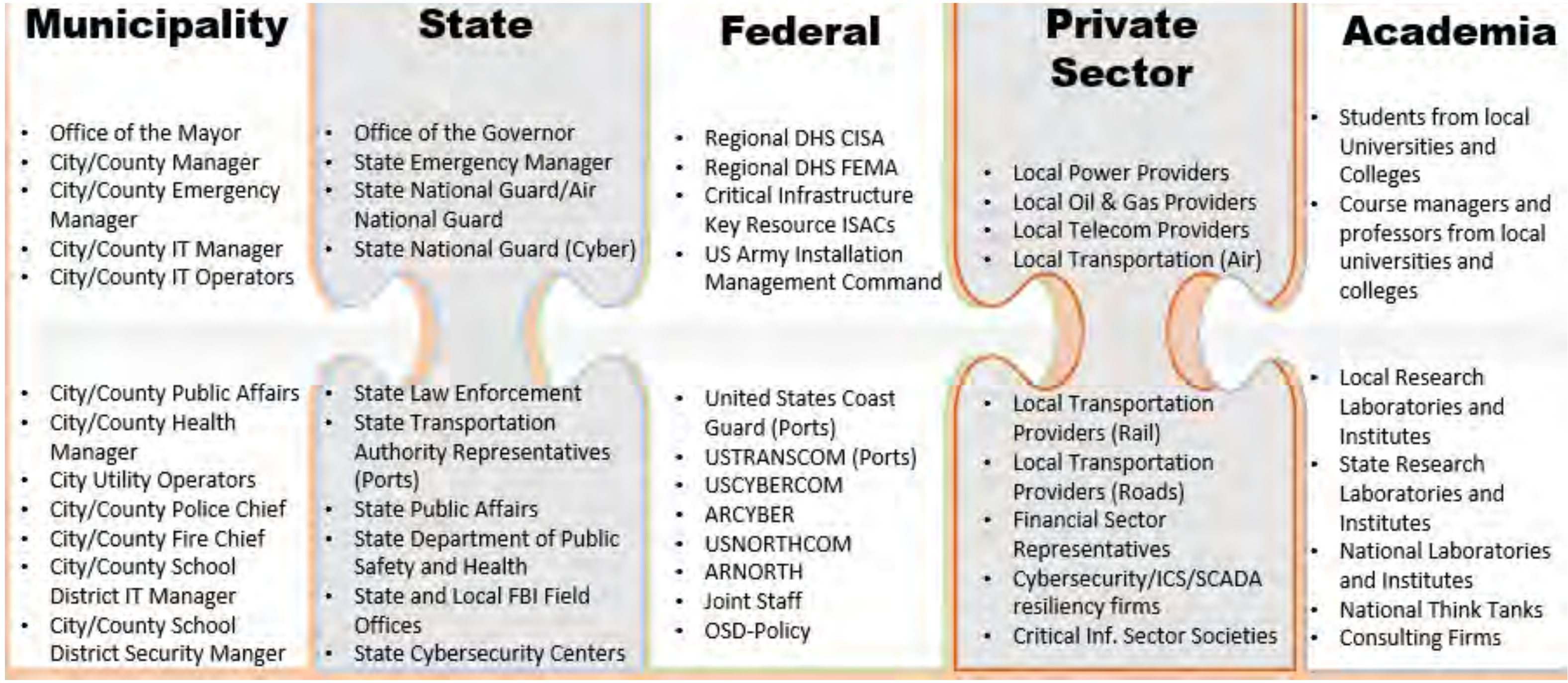
Governor, State Police, State EMS, State Guard

Electrical, Water/Sewer, Natural Gas, Rail, Hospitals, Bridges, Port Authority, Internet Providers, Commercial Communications, Financial Institutes, etc.

Mayor's Office, School Board, Transportation, City IT

Local Emergency Management, Local Law Enforcement, Local Fire and Rescue, Local Paramedics

Tactical Stakeholders-Cont.



Municipality	State	Federal	Private Sector	Academia
• Office of the Mayor • City/County Manager • City/County Emergency Manager • City/County IT Manager • City/County IT Operators	• Office of the Governor • State Emergency Manager • State National Guard/Air National Guard • State National Guard (Cyber)	• Regional DHS CISA • Regional DHS FEMA • Critical Infrastructure Key Resource ISACs • US Army Installation Management Command	• Local Power Providers • Local Oil & Gas Providers • Local Telecom Providers • Local Transportation (Air)	• Students from local Universities and Colleges • Course managers and professors from local universities and colleges
• City/County Public Affairs • City/County Health Manager • City Utility Operators • City/County Police Chief • City/County Fire Chief • City/County School District IT Manager • City/County School District Security Manger	• State Law Enforcement • State Transportation Authority Representatives (Ports) • State Public Affairs • State Department of Public Safety and Health • State and Local FBI Field Offices • State Cybersecurity Centers	• United States Coast Guard (Ports) • USTRANSCOM (Ports) • USCYBERCOM • ARCYBER • USNORTHCOM • ARNORTH • Joint Staff • OSD-Policy	• Local Transportation Providers (Rail) • Local Transportation Providers (Roads) • Financial Sector Representatives • Cybersecurity/ICS/SCADA resiliency firms • Critical Inf. Sector Societies	• Local Research Laboratories and Institutes • State Research Laboratories and Institutes • National Laboratories and Institutes • National Think Tanks • Consulting Firms

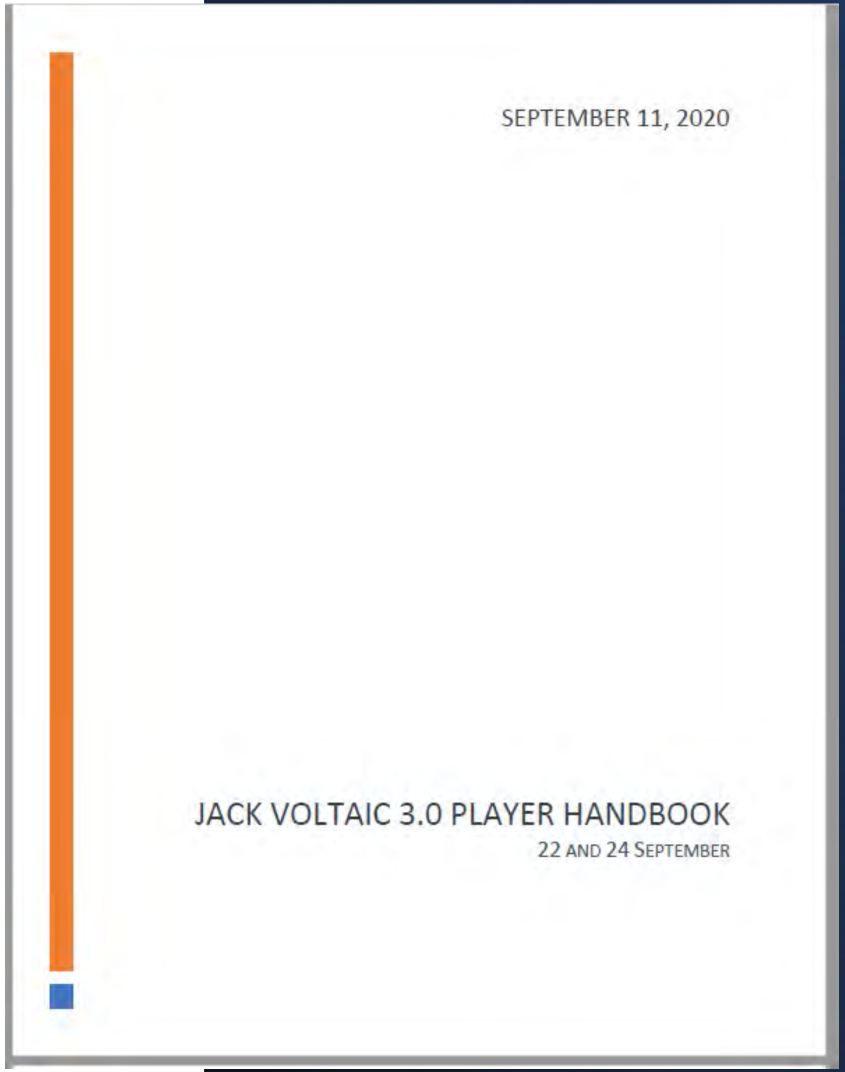
- **Depended on who showed up**
  - May have excluded organizations that would have had a significant role
  - Scenario targeted organizations: Public safety, police, fire, emergency mgt were not “told” to participate
  - Specific lifeline being hit should be involved
  - Desire representation from diverse sectors

Lessons Learned and New Opportunities

- HSEEP
- Exercise Control
- Exercise Approach and Planning
- Forced distribution, Forced Win
- Data Collection
- New Partnerships

HSEEP

- Attempted HSEEP
- Dynamic situation
- Planning changes made HSEEP process difficult to follow
- Players' Handbook – Combined JELC and HSEEP



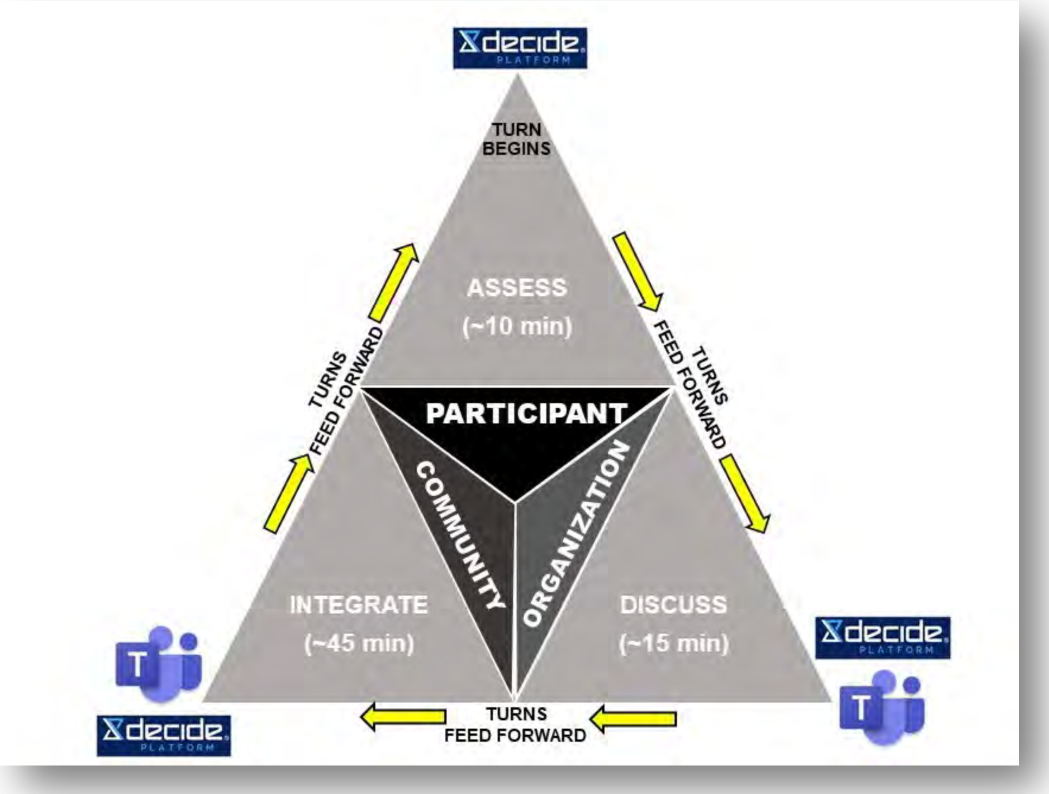
SEPTEMBER 11, 2020

JACK VOLTAIC 3.0 PLAYER HANDBOOK

22 AND 24 SEPTEMBER

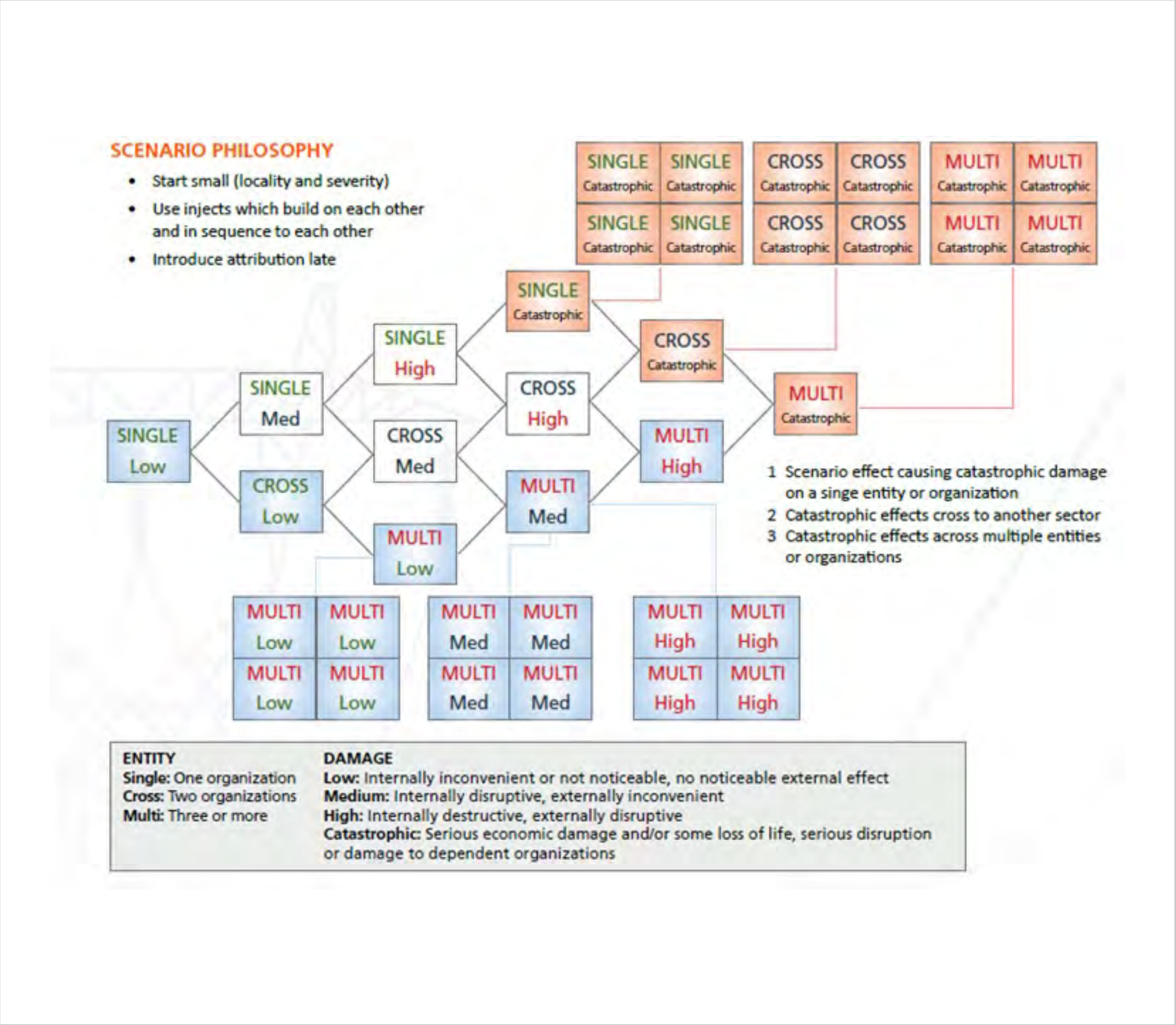
Exercise Control

- Learned how to conduct Distributed Exercises
- Developed a repeatable process, combining MS Teams and DECIDE®
- Enabled engagement at multiple levels and lifelines
- Flow Triangle - huge win



Exercise Approach and Planning

- Inject/Event topology for maximum impact and engagement
- Currently used with other exercise planning teams
- Exercise would not have happened without DECIDE®



SCENARIO PHILOSOPHY

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

1 Scenario effect causing catastrophic damage on a singe entity or organization
2 Catastrophic effects cross to another sector
3 Catastrophic effects across multiple entities or organizations

ENTITY
Single: One organization
Cross: Two organizations
Multi: Three or more

DAMAGE
Low: Internally inconvenient or not noticeable, no noticeable external effect
Medium: Internally disruptive, externally inconvenient
High: Internally destructive, externally disruptive
Catastrophic: Serious economic damage and/or some loss of life, serious disruption or damage to dependent organizations

Forced Distribution/Forces Win

- JV was at serious risk
- Didn't quit! Did something to keep moving
- Jack Pandemus saved Jack Voltaic
- JP testbed to incorporate other scenarios
  and distributed resources

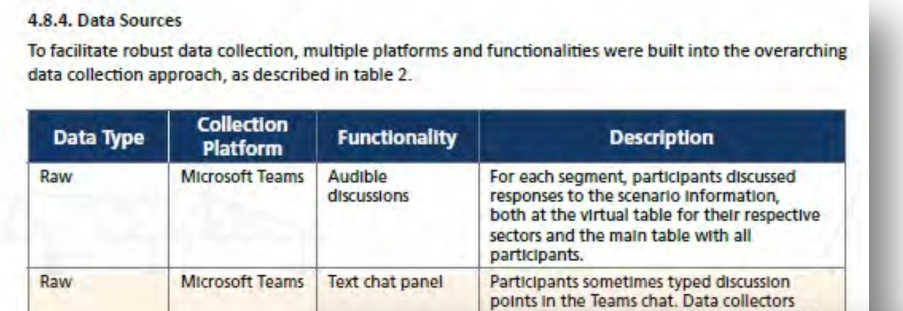
Jack Pandemus

Mini-Exercise 9 June 2020

ARMY CYBER INSTITUTE AT WEST POINT
Jack Voltaic® 3.0
NUARI
NUARI
Norwich University Applied Research Institutes
FTI CONSULTING
Provatek
Technology Proven

Data Collection

- Distributed Data Collection
- Observer coding (meta-tagging)
- Questionnaires, Surveys, Observations

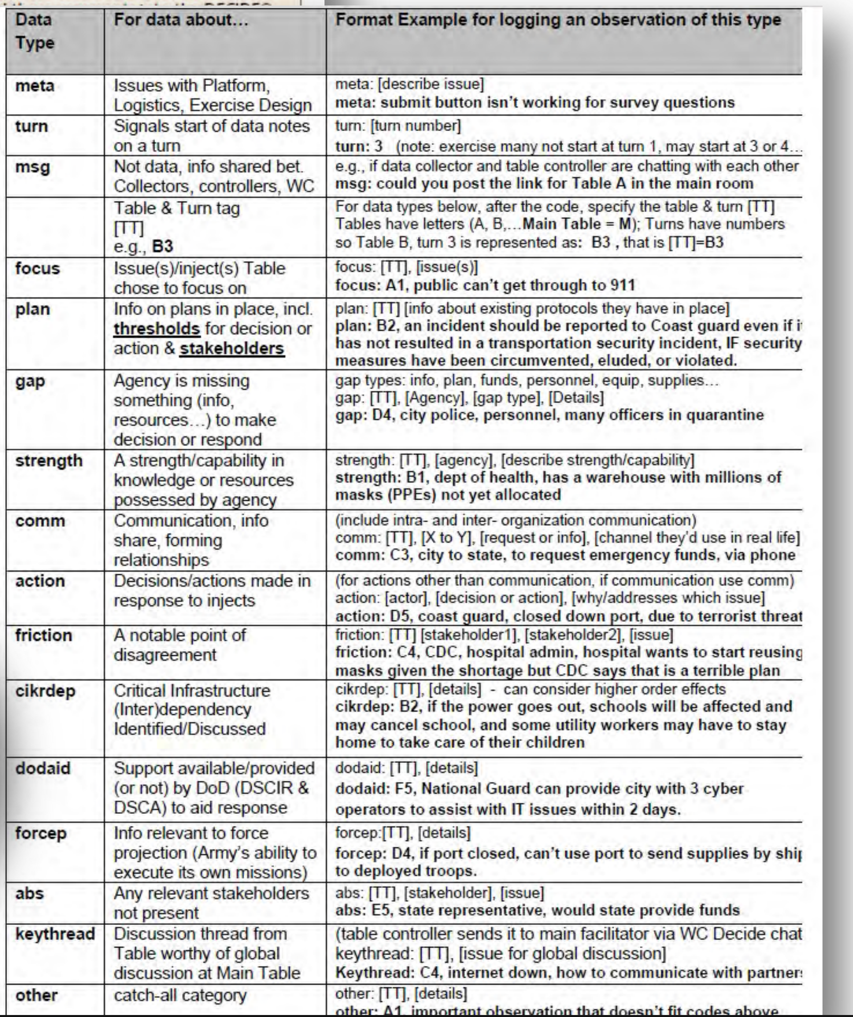


4.8.4. Data Sources

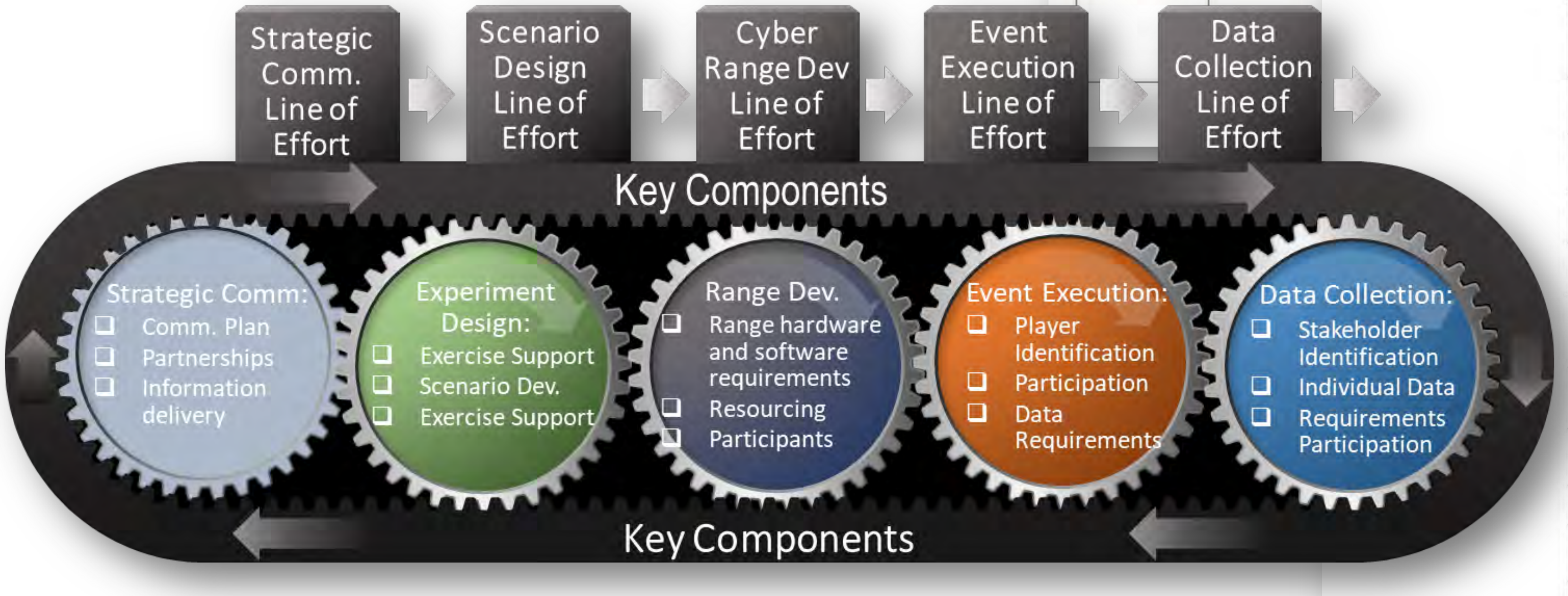
To facilitate robust data collection, multiple platforms and functionalities were built into the overarching data collection approach, as described in table 2.

Data Type	Collection Platform	Functionality	Description
Raw	Microsoft Teams	Audible discussions	For each segment, participants discussed responses to the scenario information, both at the virtual table for their respective sectors and the main table with all participants.
Raw	Microsoft Teams	Text chat panel	Participants sometimes typed discussion points in the Teams chat. Data collectors
Raw	DECIDE®		
Structured	DECIDE®		
Structured	DECIDE®		

Data Codes

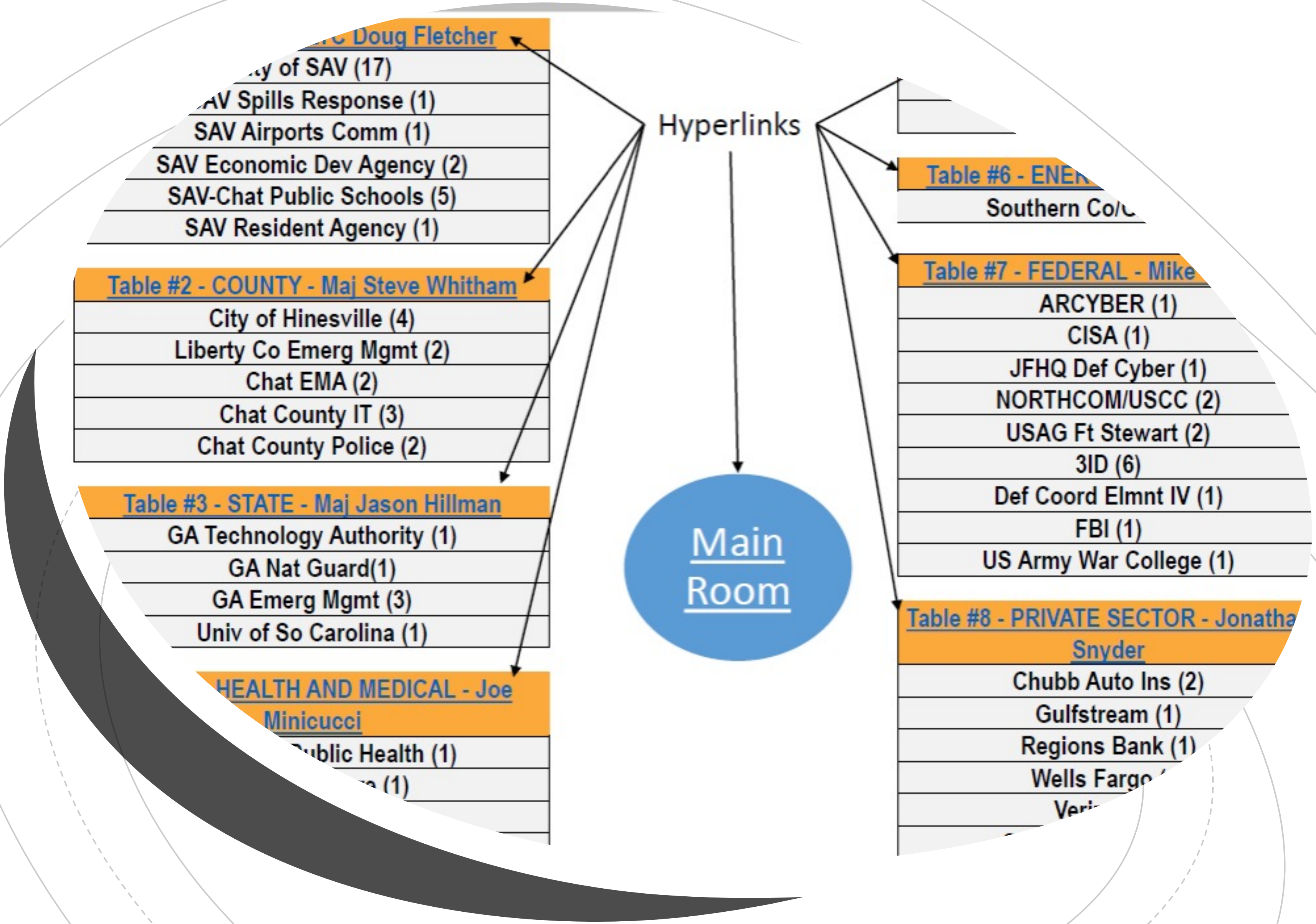


Data Type	For data about…	Format Example for logging an observation of this type
meta	Issues with Platform, Logistics, Exercise Design	meta: [describe issue] **meta: submit button isn't working for survey questions**
turn	Signals start of data notes on a turn	turn: [turn number] **turn: 3** (note: exercise many not start at turn 1, may start at 3 or 4…
msg	Not data, info shared bet. Collectors, controllers, WC	e.g., if data collector and table controller are chatting with each other **msg: could you post the link for Table A in the main room**
	Table & Turn tag [TT] e.g., **B3**	For data types below, after the code, specify the table & turn [TT] Tables have letters (A, B,…**Main Table = M**); Turns have numbers so Table B, turn 3 is represented as: **B3** , that is [TT]=B3
focus	Issue(s)/inject(s) Table chose to focus on	focus: [TT], [issue(s)] **focus: A1, public can't get through to 911**
plan	Info on plans in place, incl. **thresholds** for decision or action & **stakeholders**	plan: [TT] [info about existing protocols they have in place] **plan: B2, an incident should be reported to Coast guard even if i has not resulted in a transportation security incident, IF security measures have been circumvented, eluded, or violated.**
gap	Agency is missing something (info, resources…) to make decision or respond	gap types: info, plan, funds, personnel, equip, supplies… gap: [TT], [Agency], [gap type], [Details] **gap: D4, city police, personnel, many officers in quarantine**
strength	A strength/capability in knowledge or resources possessed by agency	strength: [TT], [agency], [describe strength/capability] **strength: B1, dept of health, has a warehouse with millions of masks (PPEs) not yet allocated**
comm	Communication, info share, forming relationships	(include intra- and inter- organization communication) comm: [TT], [X to Y], [request or info], [channel they'd use in real life] **comm: C3, city to state, to request emergency funds, via phone**
action	Decisions/actions made in response to injects	(for actions other than communication, if communication use comm) action: [actor], [decision or action], [why/addresses which issue] **action: D5, coast guard, closed down port, due to terrorist threat**
friction	A notable point of disagreement	friction: [TT] [stakeholder1], [stakeholder2], [issue] **friction: C4, CDC, hospital admin, hospital wants to start reusing masks given the shortage but CDC says that is a terrible plan**
cikrdep	Critical Infrastructure (Inter)dependency Identified/Discussed	cikrdep: [TT], [details] - can consider higher order effects **cikrdep: B2, if the power goes out, schools will be affected and may cancel school, and some utility workers may have to stay home to take care of their children**
dodaid	Support available/provided (or not) by DoD (DSCIR & DSCA) to aid response	dodaid: [TT], [details] **dodaid: F5, National Guard can provide city with 3 cyber operators to assist with IT issues within 2 days.**
forcep	Info relevant to force projection (Army's ability to execute its own missions)	forcep:[TT], [details] **forcep: D4, if port closed, can't use port to send supplies by shi to deployed troops.**
abs	Any relevant stakeholders not present	abs: [TT], [stakeholder], [issue] **abs: E5, state representative, would state provide funds**
keythread	Discussion thread from Table worthy of global discussion at Main Table	(table controller sends it to main facilitator via WC Decide chat keythread: [TT], [issue for global discussion] **Keythread: C4, internet down, how to communicate with partner**
other	catch-all category	other: [TT], [details] **other: A1, important observation that doesn't fit codes above**



New Partnerships

The planning and exercise method encouraged new cross-functional relationships and discussions



C Doug Fletcher
ty of SAV (17)
AV Spills Response (1)
SAV Airports Comm (1)
SAV Economic Dev Agency (2)
SAV-Chat Public Schools (5)
SAV Resident Agency (1)

Table #2 - COUNTY - Maj Steve Whitham
City of Hinesville (4)
Liberty Co Emerg Mgmt (2)
Chat EMA (2)
Chat County IT (3)
Chat County Police (2)

Table #3 - STATE - Maj Jason Hillman
GA Technology Authority (1)
GA Nat Guard(1)
GA Emerg Mgmt (3)
Univ of So Carolina (1)

HEALTH AND MEDICAL - Joe Minicucci
ublic Health (1)
(1)

Hyperlinks

Main Room

Table #6 - ENER
Southern Co/C

Table #7 - FEDERAL - Mike
ARCYBER (1)
CISA (1)
JFHQ Def Cyber (1)
NORTHCOM/USCC (2)
USAG Ft Stewart (2)
3ID (6)
Def Coord Elmnt IV (1)
FBI (1)
US Army War College (1)

Table #8 - PRIVATE SECTOR - Jonatha Snyder
Chubb Auto Ins (2)
Gulfstream (1)
Regions Bank (1)
Wells Fargo
Veri

Questions/Wrap Up

For more info on DECIDE® browse to:
https://nuari.net/decide/

- Joe Minicucci – jminicu2@norwich.edu
- Tom Muehleisen – tmuehlei@norwich.edu
- Steven Whitham - steven.whitham@westpoint.edu

Lunch

See you back here at 12:30 EDT

NUARI 1819
Norwich University Applied Research Institutes

JACK VOLTAIC

conference series

Prepare | Prevent | Respond | Report

June 23, 2021

Technology Integration and Cyber Resilience

NUARI 1819
Norwich University Applied Research Institutes

THE CITADEL

ARMY CYBER INSTITUTE AT WEST POINT

GEORGIA CYBER CENTER
AUGUSTA UNIVERSITY

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Welcome to the Conference

9:00 – 9:15 am	Welcome & Introduction	Phil Sussman (President, NUARI)
9:15 – 9:30 am	Jack Voltaic 3.0 Background and NUARI Role	LTC Erica Mitchell (ACI)
9:30 – 10:10 am	Critical Infrastructure and Cyber Resilience	Bryson Bort (Scythe)
10:10 – 10:20 am	Break	
10:20 – 11:00 am	Using Analytic Tools to Identify Critical Infrastructure Dependencies using AHA	Tom Muehleisen (NUARI) Ryan Hruska (INL) MAJ Steve Whitham (ACI)
11:00 – 11:45 am	Challenges of Distributed Critical Infrastructure Exercises – Lessons Learned	Tom Muehleisen (NUARI) Joe Minicucci (NUARI) MAJ Steve Whitham (ACI)
11:45 am – 12:30 pm	Lunch break	
12:30 – 2:00 pm	ACI Technical Integration Project Background and Development Process	MAJ Steve Whitham (ACI) Mike Schulz (NUARI) TR Staake (NUARI) Evan Owen (52inc)
2:00 – 2:10 pm	Break	
2:10 – 3:30 pm	Technical Integration Proof of Concept Demo & Mini Exercise	Mike Schulz (NUARI) Evan Owen (52inc) MAJ Steve Whitham (ACI)
3:30 – 3:50 pm	Questions, Discussion, and Feedback	Kristen Pedersen (NUARI)
3:50 - 3:55 pm	Next Conference: Georgia Cyber Center - **Developing a Unified Approach to Critical Infrastructure**	Eric Toler (GCC) MAJ Steve Whitham (ACI)
3:55 - 4:00 pm	Closing	Kristen Pedersen (NUARI)

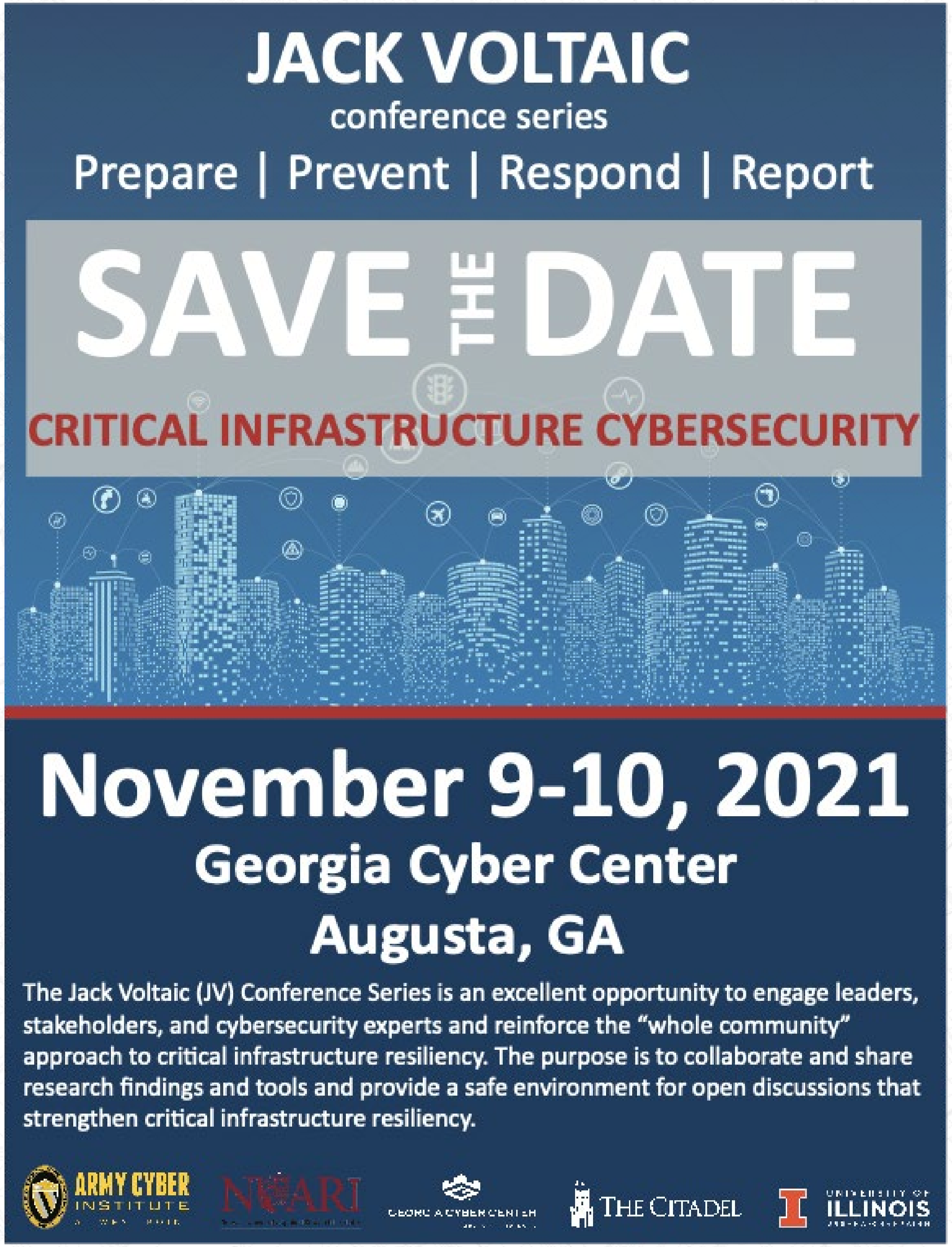
Live Demo

Questions?

T. Eric Toler

Executive Director

GEORGIA
CYBER CENTER



JACK VOLTAIC

conference series

Prepare | Prevent | Respond | Report

SAVE THE DATE

CRITICAL INFRASTRUCTURE CYBERSECURITY

November 9-10, 2021

Georgia Cyber Center

Augusta, GA

The Jack Voltaic (JV) Conference Series is an excellent opportunity to engage leaders, stakeholders, and cybersecurity experts and reinforce the "whole community" approach to critical infrastructure resiliency. The purpose is to collaborate and share research findings and tools and provide a safe environment for open discussions that strengthen critical infrastructure resiliency.

ARMY CYBER INSTITUTE

GEORGIA CYBER CENTER

THE CITADEL

UNIVERSITY OF ILLINOIS

Thank you for attending!

NUARI

1819

Norwich University Applied Research Institutes

nuari.net

THE CITADEL

ARMY CYBER INSTITUTE AT WEST POINT

GEORGIA CYBER CENTER
AUGUSTA UNIVERSITY

UNIVERSITY OF ILLINOIS
URBANA-CHAMPAIGN