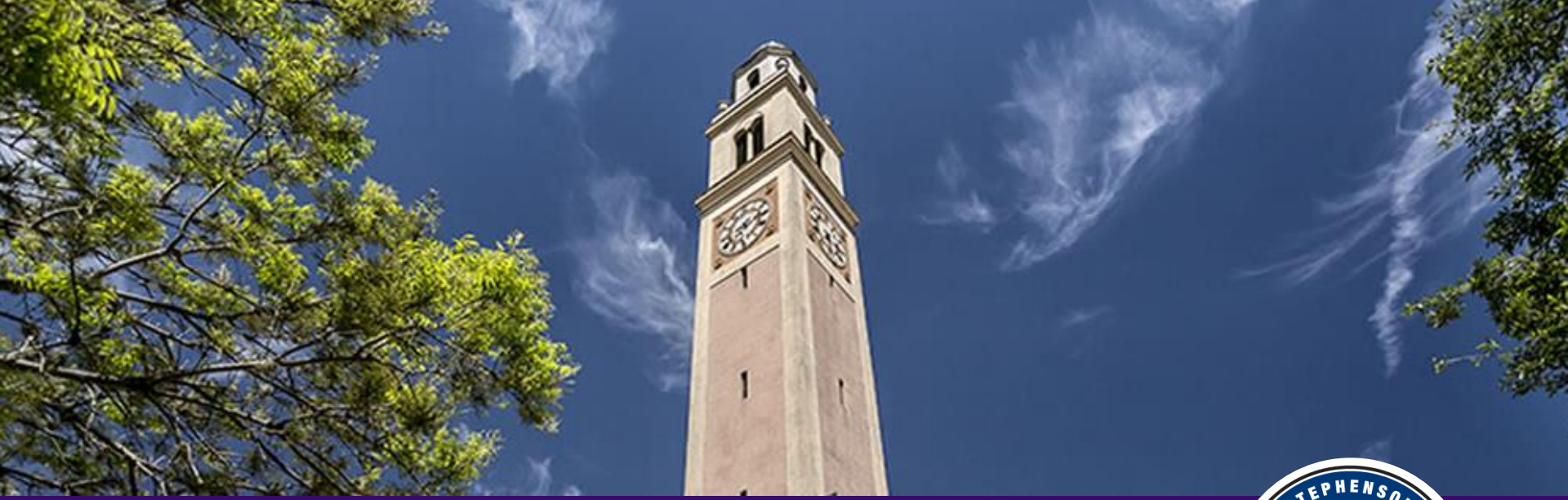


LSU | Stephenson National Center for Security Research and Training

Cyber Policy and Response Capabilities

Brant Mitchell
Director of Operations

SNCSRT Organizational Chart

Units and Missions

SNCSRT

TTCRC
Research Unit

SDMI
Research Unit

NCBRT
Research & Training Unit

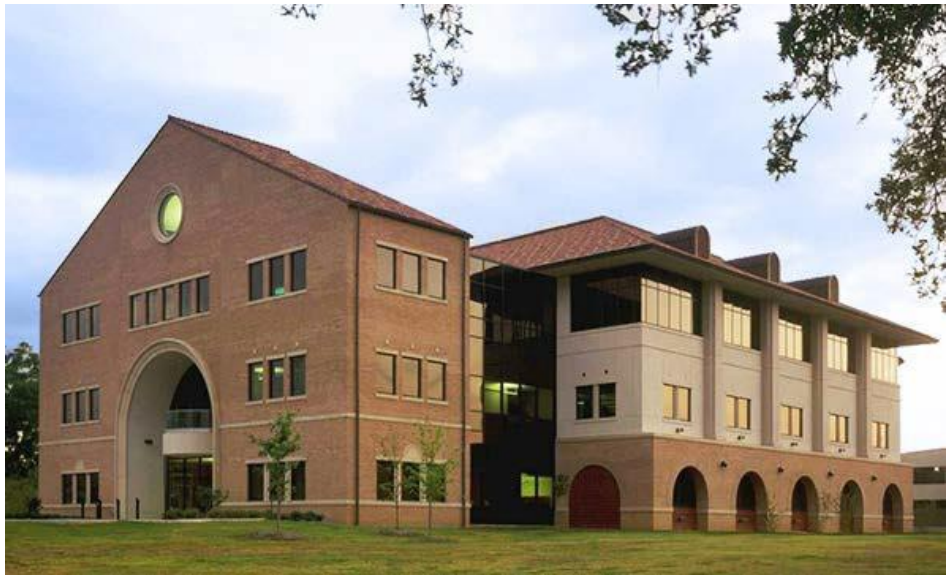
NCDF
Service Unit

LEO
Service Unit

FETI
Training Unit

Stephenson Technology Corporation

- Non-profit, 501(c)(3) Professional Services R&D Enterprise
- Operates as standalone corporation, wholly owned by LSU
- Focus: Solutions to DoD, DHS, IC, and Federal markets
- Fully compliant Federal contractor.
- TS Facility Clearance
- TS (full scope poly) cleared employees
- On-campus Headquarters/On-site Support
- Member, Cyber and Emerging Technologies Division Advisory Board, *National Defense Industrial Association*



STC STEPHENSON TECHNOLOGIES CORPORATION
AN LSU 501(C)3 AFFILIATE

NDIA Member, Cyber and Emerging Technologies Division Advisory Board

Current Clients, Partners, and Customers

DOD RESEARCH

AFRL

ASDR&E

ONI

NRL

NRO

JCTD w/ ASDR&E

COMBATANT COMMANDS

USCYBERCOM

ASDR&E

EUCOM

AFRICOM

SOUTHCOM

SOCOM

STATE / REGIONAL PARTNERS

GOHSEP

ASDR&E

LADOJ

LA-SAFE

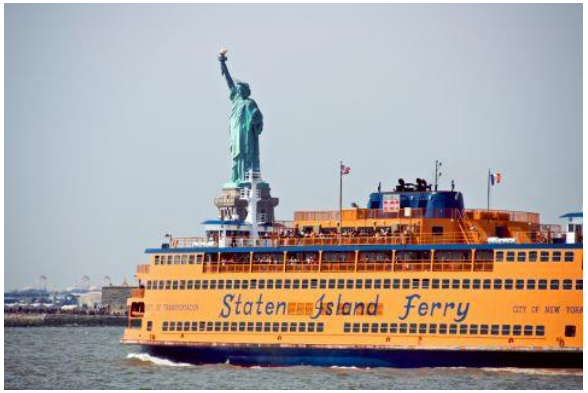
Cyber Based Table Top Exercises

Port of NY/NJ Cybersecurity Tabletop Series

TTX Exercise 1 – Bulk Storage

TTX Exercise 2 – Containers

MARITIME SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE



TTX Exercise 3 – Passenger Ferries

TTX Exercise 4 – Gulf of Mexico

LSU

Lessons Learned

- Lack of Trust Between Private Sector and Government
- No defined mechanism to identify and communicate Cyber risks or threat levels
- MARSEC may not be appropriate for cyber
- Information sharing is uneven across the sector as well as between sectors
- Vendors may represent a challenge to managing cybersecurity risks

Lessons Learned

- Operational Staff may not have the knowledge or training to immediately recognize a cyber incident
- Cyber incident reporting requirements and procedures are unclear
- Cyber incident response capabilities vary across private sector organizations
- Safety culture, operational culture must extend to cyber space

Current Operational Environment

- National Cybersecurity Protection Act 2014
  - Codifies NCCIC's cyber operations center into law
  - Directs NCCIC to formalize information sharing, provide technical assistance, risk management support, and incident response activities
- Presidential Policy Directive 41 – Cyber Incident Coordination
  - Cyber Unified Coordination Group
  - 3 Lines of Efforts
    - Threat Response Activities – FBI NCIJTF
    - Asset Response Activities – DHS NCCIC
    - Intelligence Support – DNI Cyber Threat Intelligence Integration Center

Current Operational Environment - DHS

- National Cybersecurity and Communications Integration Center
  - NCCIC Operations & Integration (NO&I)
    - 24/7 Situational Awareness
  - Threat Detection and Analysis
    - US-CERT
    - ICS-CERT
  - Response
    - HIRT
  - National Communications Center (NCC)
  - National Cybersecurity Assessment and Technical Services (NCATS)

Current Operational Environment - DHS

- U.S. Coast Guard
  - Cyber Strategy – 2015
  - Navigation and Vessel Inspection Circulars – 05-17
    - USCG Interpretation of MTSA for Cyber
    - Governance and Risk Management for Cyber

Current Operational Environment - DOJ

- 91 Computer Crime Task Forces across the United States
- Consists of Federal, State and Local cyber experts

Current Operational Environment - DoD

- Cyber Command
  - 13 Cyber Protection Teams (CPTs)
- NORTHCOM
  - OPCON 1 CPT
- National Guard Bureau
  - 11 Cyber Protection Teams
    - 10 deployed to the States
    - 1 maintained at NGB with full-time manning

Trump Administration Cyber Initiatives

- Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  - Signed May 2017
  - Requires Federal agencies to use the NIST cybersecurity framework to guide internal risk assessments
  - Accelerates the government's move toward the use of shared information systems and security infrastructure, to include cloud computing
  - Formalizes cybersecurity efforts under the authority of the President
- Vulnerabilities Equities Process
  - November 2017

Trump Administration FY-19 Budget Priorities

- Increase for DOD cyber efforts and capabilities – total $8 billion
- Establishes policy for the Pentagon's use of offensive cyber capabilities
- Creates a new Office of Cybersecurity, Energy Security and Emergency Response within the Department of Energy
  - Additional $96 million in budget authority
- $32 million expansion of the DHS 24/7 Cyber Watch
  - Increase tracking of cyber incidents and advanced warning

HR 3101 – Strengthening Cybersecurity Information Sharing and Coordination in our Ports Act of 2017

- Introduced by Representative Torres from California
- Directs DHS to:
  - Develop and implement a maritime cybersecurity risk assessment model to evaluate current and future cybersecurity risks
  - Seek input from at least one ISAO representing maritime interest
  - Establish voluntary reporting guidelines
  - Requests that the National Maritime Security Advisory Committee report and make recommendations to DHS about enhancing information sharing.

HR 3101 – Strengthening Cybersecurity Information Sharing and Coordination in our Ports Act of 2017

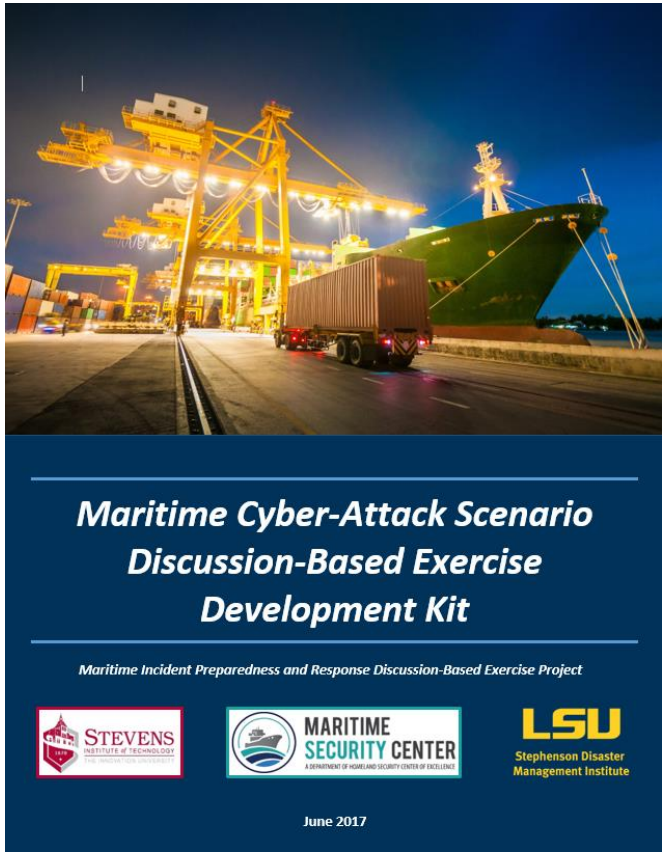
- Directs DHS, through the US Coast Guard to:
  - Direct each AMSAC to facilitate the sharing of information on addressing port-specific cybersecurity vulnerabilities
  - Requires that all MTSA required facility owners and operators to include mitigation measures to prevent, manage and respond to cyber threats and vulnerabilities in the Facility Security Plans

Federal Cyber Policy Overview

- Focused on Information Sharing
- Implementation of the NIST Cybersecurity Framework
- Providing Technical Assistance to 16 Critical Infrastructure Sectors
- Continuing to build robust capabilities primarily designed to protect the various Federal Information Systems but can be leveraged to support SLTT and Private Sectors

Exercise Development Kit

1. List of Potential Players
2. Core Capability Alignment
3. Recommended Objectives
4. Scenario Builder
5. Facilitator Guide
6. Sample Exercise Outline



Brant Mitchell

bmitch9@lsu.edu