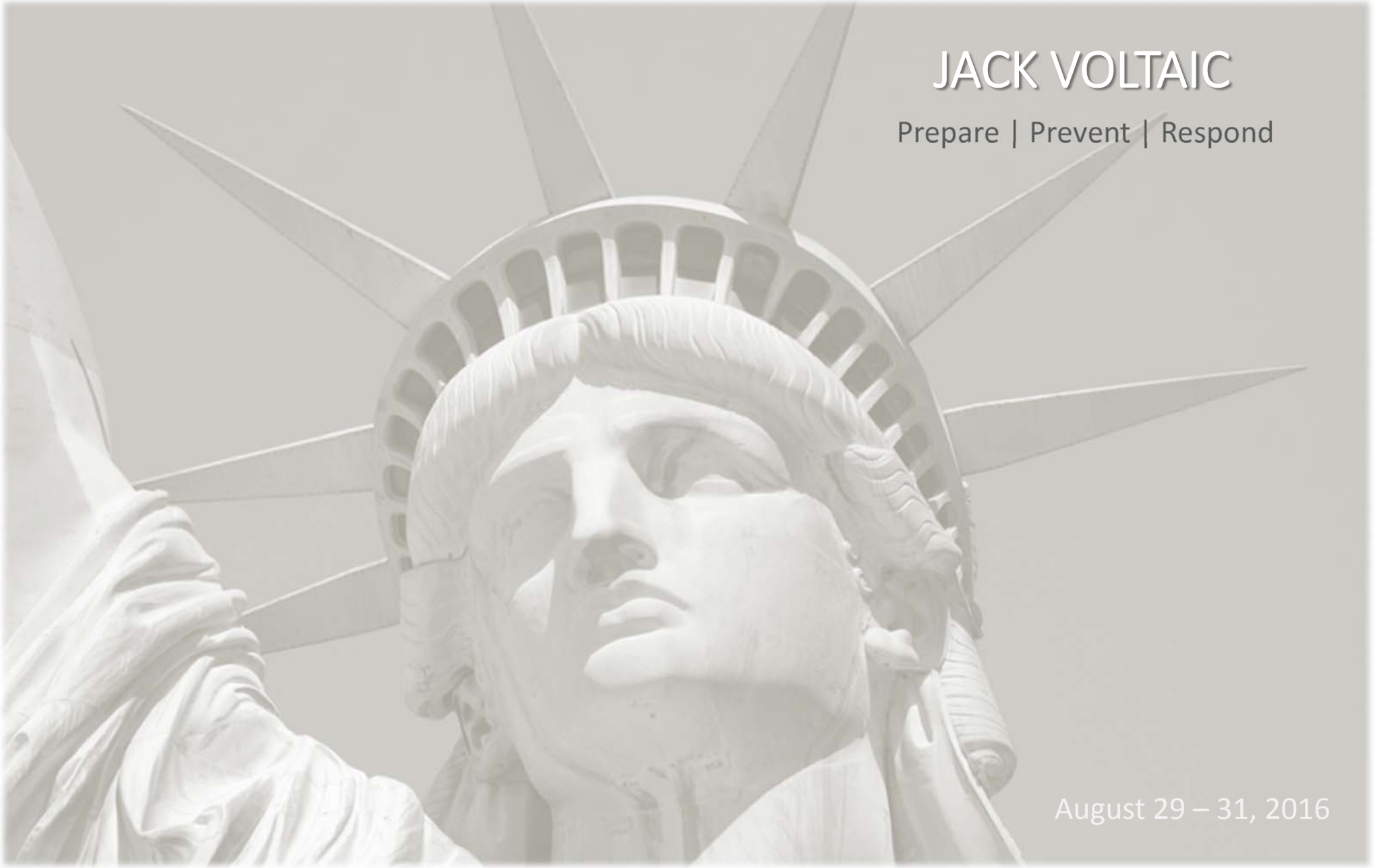


JACK VOLTAIC

Prepare | Prevent | Respond

August 29 – 31, 2016

Jack Voltaic

Prepare | Prevent | Respond

Executive Summary

During the period of August 29-31 2016, the Army Cyber Institute (ACI) in conjunction with Citigroup, executed a major city, multi sector, public private cyber exercise called **Jack Voltaic** (JV). It was the first step in building a framework to prepare, prevent, and respond to multi-sector cyber-attacks on major cities. Jack Voltaic was a research experiment in the form of a cyber exercise that involved players from multiple sectors, including first responders, emergency management, transportation, telecommunications, power, water, finance and healthcare. The exercise included two parallel tracks consisting of: 1) an on-range network defender versus attacker live-fire exercise (LFX), and 2) a facilitated table-top exercise (TTX) among sector leadership focused on events occurring in the virtual range play. The goal was to exercise and observe a city's ability, to collaborate in a coordinated respond in any cyber-attacks.

137 Participants
25 Organizations

"Bringing together the Right People to Solve the Right Problems"

Purpose:

In general there are three-levels (listed below) of cyber-exercises conducted. All categories of cyber exercises are necessary and serve a particular objective. Jack Voltaic was focused on the local-level city response.

- **National** (strategically focused, e.g. Cyber Guard, Cyber Storm, Cyber Shield and multiple-sector)
- **Regional** (multi-state, e.g. National Guard, Quantum Dawn, Grid-Ex - critical infrastructure-sector specific and multiple-sector)
- **Local-level** (table top exercise style, e.g. city, specific to organizational training objectives)

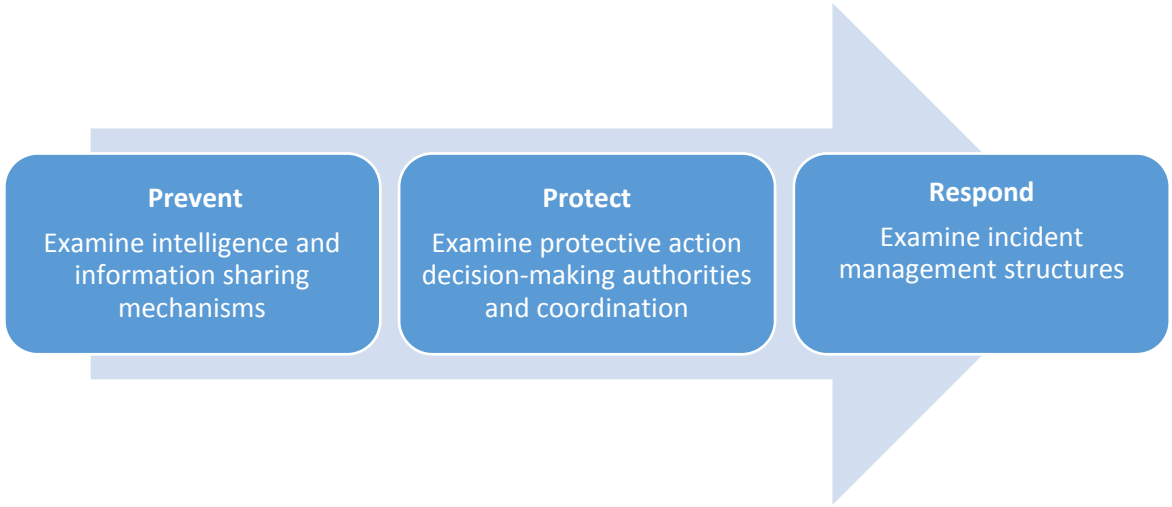
Scope:

To develop a small exercise event, demonstrating a cyber-attack in New York City (NYC), impacting multiple sectors and to exercise a city's ability to respond to the attack. All pertinent federal and state level agencies are consulted and encouraged to observe, but the focus remains on the city.

Objectives:

The main objective is to identify a framework and the opportunity to rehearse coordinated responses by any city to cyber incidents that affect multiple sectors. Secondarily this experimental exercise will provide a venue that enables participants to gain exposure, train players and/or evaluate response.

- Focus on NYC Emergency Management prioritization and coordination of recovery effort.
- Examine interdependencies, identify the potential gaps between sectors and challenges to cyber security.
- Identify strengths and weaknesses and potentially draw out best practices for improving system security and incident response.
- Provide awareness and insight to challenges facing sectors as it pertains to responding to a cyber-attack.



Background:

Innovate

- The Army Cyber Institute (ACI) is charged with providing innovative ideas to the Army, the Department of Defense (DoD) and the Nation in order to address future cyber-related challenges. One of the challenges the ACI is exploring is urban dense areas (megacities) through the study of cyber-related exercises and critical infrastructure.
- The ACI is exploring the current model of Regional Mutual Assistance Groups (RMAGs) an energy sector' framework to provide operational and technical assistance to meet cyber capability needs during a large-scale cyber event or attack on the energy sector. This same capability does not exist within the cyberspace domain. During an incident impacting the cyberspace domain the scope of requirements for cyber capabilities to respond to cyber events remain a challenge.

Experiment

- On April 08, 2016, the ACI conducted a Cyber Mutual Assistance Workshop (CMAW). The workshop provided an opportunity for practitioners and experts from across the public and private sectors to gather and collaborate in a holistic approach to examine issues concerning the energy sector. One of the objectives was to conduct a follow-on experiment to examine interdependencies among critical infrastructure sectors.
- The ACI wanted to conduct and expirement to further examine mutual assistance from the angle of preparation, prevention, and response using a cyber exercise. While the ACI has resources towards the study and research of public-private cyber-related exercises, it does not have the ability to develop and run exercises regularly. The ACI's mission encompasses developing impactful partnerships accross academia, industry and government to develop intellectual capital for advancing the body of knowledge. The ACI needed to leverage the broader community.

Partner

- The ACI leveraged an ongoing collaboration with Citigroup's Global Cyber Threat Exercise Team (Citi-GCTET) to develop a small, multi-sector exercise. Citi's GCTET is responsible for the development, planning, execution, reporting and communication of strategic, tactical and technical cyber threat exercises and war games. In May 2016, Citi's GCTET began co-leading the development of Jack Voltaic with the ACI.
- Over the course of the four months, ACI consulted across relevant federal, state and local entities to ensure diligence. Jack Voltaic is inspired by the 2014 New York City (NYC) Partner Cyber TTX, which was an exercise led and executed by the Department of Homeland Security (DHS) alongside the Federal Bureau of Investigation (FBI).
- Reference: DHS Situation Manual for 2014, NYC City Partner TTX After Action Review, contact DHS-NCCIC-National Cyber Exercise and Planning Program (NCEPP).

Timeline:

Cyber Mutual Assistance Workshop

April 08, 2016 at the Army Cyber Institute, West Point, NY.

_____

The workshop was led and facilitated by the ACI, the Electric Infrastructure Security Council and Carnegie Mellon University. It provided an opportunity for experts and practitioners from across the public and private sectors to gather and collaborate in a holistic approach to examine issues concerning the energy sector.

Spawned the idea to develop an experiment.

Initial Planning

May 16, 2016 at the Army Cyber Institute, West Point, NY.

_____

The goal of this meeting was to begin the development of the exercise scope, scenario, and objectives. In addition, the official exercise planning committee was solidified.

Midterm Planning

July 06, 2016 at the NYC Emergency Management, Brooklyn, NY.

_____

The goal of this meeting was to conduct a comprehensive review of the overall JV scenario. Begin developing injects and synchronize the components (LFX and TTX) with identified cyber-attack events. Ensure all planners have a common understanding of the rules of engagement and exercise flow.

Final-Planning

August 04, 2016, at the FDNY Operation's Center, Brooklyn, NY.

_____

The goal of this meeting was is to conduct a final review of the overall JV scenario. Discuss updates to the action items noted during the mid-term planning meeting. Ensure all planners have a common understanding of the rules of engagement of both the LFX and TTX flow. Verify any additional logistical or training requirements for the exercise.

July 27 – 29, conduct LFX range orientations

Execution

August 29 - 31 2016 at the HNA Palisades Conference Center, Palisades, NY.

_____

August 1-12 conduct LFX Blue Teams range reconnaissance period

August 8 – Range Freeze

August 15-26 conduct LFX Red Teams Range Recce period

Design Concept:

This exercise was inspired by existing cyber exercise frameworks but did not follow any specific one. Cyber exercises are typically hindered by being either overly technical or too high-level policy-wise where the managers/operators and the technical personnel are not in the same room. Our goal in this experiment was to ensure the TTX participants interacted with the technical exercise (LFX) participants. In general there are three levels of players involved in an exercise. These players are divided into three categories. Jack Voltaic focused on categories one and two.

- Category-3: Senior Executives
- Category-2: Mid-level management
- Category-1: Operational – Analysts and operators

Jack Voltaic was designed to incorporate and correlate components of both the 1) LFX and 2) TTX. Both components (LFX, TTX) are considered cyber simulations and vary depending on capability. Both promote exposure and opportunities to conduct collective cybersecurity training and enhance cross-sector information sharing practices. Developing the exercise in this manner helped ensure there was coordination both at the technical level of information sharing of threats and communication of effects and risk with the management level participating in the TTX. LFX participants were exposed to threat tactics, tools and shared techniques.

Planning team from L to R: Chief Warrant Officer 3 Judy Esquibel (ACI), Scott Hagerty (CITI), Dr. Fernando Maymi (ACI), Anthony Vitello (CITI), John Cosgrove (CITI), Irina Garrido (ACI), Stephen Ross (CITI), Arielle Budoff and Brian Wilson (CITI)

Component 1: Live-Fire-Exercise (LFX)

Correlated

- Consisted of an on-range network virtual range environment
- Network defenders (blue team) were responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers.
- The blue team consisted of Citigroup, FDNY, NYC DEP, Con Edison and AT&T and were arranged to defend three notional networks: Financial, Government and Utility. They leveraged sensors and analysis tools on the range to detect and respond to threat activity targeting the defended network; NOT "capture the flag".
- The opposing force (OPFOR-re team) generally mount a hostile attack against blue team networks. Their objective is to improve enterprise information assurance (cyber security) or incident response to enable cyber resiliency by demonstrating the impacts of successful attacks and by demonstrating what works for defenders in an operational environment.
- The red team consisted of the United States Military Academy Cyber Competitive Team (C3T) Cadets, National Guard New York, Maryland and Con Edison.
- The white Cell is responsible for controlling and facilitating engagement between blue and red teams. Enforces the rules of the exercise.
- Has potential to incorporate other emulated critical infrastructure environments to enhance training

Component 2: Table-Top-Exercise (TTX)

- Consisted of an informal, guided conversation led by a moderator who facilitates discussion among participants
- Participants included key players (focused on local emergency responders) from NYC Emergency Management, Department of Information Technology and Telecommunications (DoITT), Police Department (NYPD), 911, Fire Department New York (FDNY) and Department of Environmental Protection (NYC DEP) that gathered in a face-to-face (U-shaped) setting and talk through expected actions for a scenario.
- The scenario used to guide the discussion was the same as that used for the LFX. Furthermore, specific events were included to strongly correlate the two tracks and ensure the decisions of the technical teams were influenced by their organizational leaders and vice versa.

Component 3: Planning Committee

- Selected planners, also known as "trusted agents" were key to the successful development and execution of this exercise.
- The committee was comprised of the emergency responder community (NYCEM, DoITT, NYPD, 911, FDNY and DEP).
- Supporting sectors were Citigroup (finance), Con Edison (power), the Metropolitan Transportation Authority or MTA (transportation), AT&T and Verizon (telecommunications), and New York University's Langone Medical Center (healthcare).
- Several emergency responder and supporting sectors planners served as subject matter experts, advisors and facilitators during the execution of the TTX and LFX.
- Planners were knowledgeable and experienced in emergency plan procedures and was involved throughout the designing, execution and evaluation of the exercise.
- In addition to the monthly (in-person) planning meetings, planners conducted bi-monthly teleconferences and leveraged the All Access Partner Network (APAN) community. APAN is a collection of communities developed to foster information and knowledge sharing between U.S. Department of Defense, multinational organizations, coalitions and non-government agencies who don't have access to traditionally restricted DOD networks

Live-Fire Exercise (LFX): The infrastructure for the LFX provided by SimSpace Corporation. This organization also facilitated the LFX and provided part of the red team for it.

- Phase 1: Breach
- Phase 2: Consolidation and initial exploitation
- Phase 3: Exploitation
- After Action Review (AAR/hotwash)

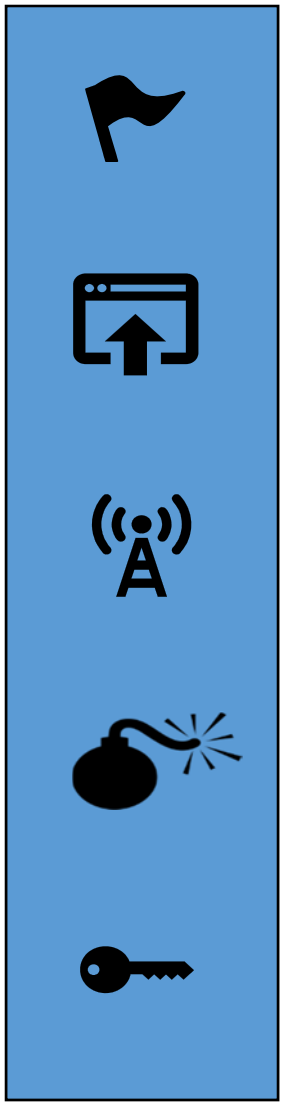
Table-Top-Exercise: The TTX was facilitated by Citigroup's Mr. John Cosgrove.

- Information Session
  - Cyber Threat Landscape Brief – "2016 Data Breach Investigation Report & Scenarios From the Field", Bhavesh Chauhan, CISSP, CISM, CISA, Verizon Security Sector Overview
- New York City emergency management procedures:
    - Henry Jackson, Deputy Commissioner, NYC Emergency Management (NYCEM)
    - Geoffrey Brown, NYC wide Chief Information Security Officer (CISO)
    - Department of Information Technology & Telecommunications (DoITT)
    - Joseph Pfeifer, Chief of Counterterrorism and Emergency Preparedness Fire Department New York (FDNY)
- Pre-Brief
  - Agenda
  - Rules of the Road
- Facilitated Table Top Discussion
  - Facilitated Discussion
    - Move 1-Immeninent Threat
    - Move 2-Response
- Hot Wash
  - Observations
  - Lessons Learned

Geoff Brown NYC wide CISO and Deputy Commissioner, DoITT

Anatomy of the Attack:

A bad day is getting worse. Seemingly random incidents continue to escalate. A major financial institution suffers system failures, sending shockwaves through the markets. Workers struggle to keep the public transportation system operating as critical control systems fail. Social media reports of terrorist attacks incite panic. The city's first response capability begins to strain. Regional medical facilities are at capacity. The media struggles to inform an increasingly concerned public. Elected leaders and emergency response leadership gather in the city's emergency operations center to analyze the situation and respond. A sinister reality emerges when a foreign terrorist group claims: the city is under siege from cyberspace. Citigroup led the design of the TTX but all ideas for this scenario came from the collective planning team.



Adversary establishes a foothold in financial sector via spear-phishing campaign disguised as sextortion.

Power sector insider installs malicious software to manipulate power substation systems.

Adversary unleashes destructive malware attack on bridge and tunnel signaling systems and water treatment plants.

Adversary agents pose as maintenance staff in One Court Square - set off a minor explosion and reveal selves as active shooters.

Adversary encrypts CRIMS database in order to delay police and fire department responses.

Way Forward:

- **Conduct After-Action-Meeting (AAM)**, date and location to be determined. The meeting will be led and facilitated by Citigroup and ACI along with key sector representatives to review and discuss observations, findings and develop a collective plan forward.

- **After-Action Report** (AAR) (30 –days). The report should include an overview of performance related to each exercise objective and associated core capabilities, while highlighting strengths and areas for improvement. Results could be used to enable planning improvement for future cyber exercises. This product will ONLY be shared with Jack Voltaic participants and will NOT be distributed to the public.

- **Academic Report** (60 – days) This will document the initial framework of a city's ability to respond to a multiple sector cyber-attack. It will capture outcomes as it pertains to the benefits of public-private partnerships, the importance of cross-sector information sharing, and the NYC Emergency Management prioritization and coordination of recovery efforts as it pertains to emergency response. This product will be distributed to a broad audience. It will be used to educate and bring awareness via a public report.

Recommended Reading:

- ***"The Big Hack - The day cars drove themselves into walls and hospitals froze. A scenario that could happen based on what already has."*** By Reeves Wiedeman, New York Magazine, June 19, 2016, http://nymag.com/daily/intelligencer/2016/06/the-hack-that-could-take-down-nyc.html

- ***"Cyber Mutual Assistance"*** – a whitepaper capturing observations and research resulting from the Cyber Mutual Assistance Workshop. By ACI, Electricity Infrastructure Security Council, and CMU-SEI-CERT, Technical Report, draft currently in edit.

- ***"Presidential Policy Directive (PPD) 41 -- United States Cyber Incident Coordination"*** -- July 26, 2016, the framework is modeled after what's done in the physical space and the NRF/PPD-8 construct. https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

    - Annex: https://www.whitehouse.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident

    - Fact Sheet: https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-0