Cyber Threats to Critical Infrastructure

Tabletop Exercise

Extensive reliance on computer networks and information systems makes the nation's critical infrastructure especially vulnerable to cyberattacks from foreign states, non-state actors, and rogue elements. Essential services across a variety of sectors – including energy, transportation, shipping, and communications – are all vulnerable to attacks, with wide-ranging ramifications for public safety, commerce, and national security.

While most organizations have some level of cyber defense in place to repel or mitigate such attacks, the next step forward in cyber defense is ensuring coordinated responses to cyber threats by all actors who could be affected – government agencies at the federal, state, and local levels, as well as privately owned infrastructure operators. Only by working together closely can these public and private sector organizations contain and mitigate the cyberattack and restore critical services.

On November 8, 2017, INSA held an exercise to test these stakeholders' responses to a cyberattack.

INSA's Exercise Was Designed to:

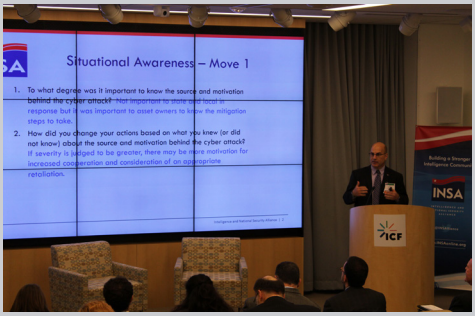
- Assess cooperation and information-sharing between intelligence, law enforcement, and the private sector;
- Identify gaps in incident response authorities, knowledge, and processes;
- Identify obstacles to prompt restoration of critical services after a cyberattack; and
- Provide insights on how government and private industry can work together to counter further cyber threats.

The Event

On November 8, 2017, INSA's Cyber Council and Domestic Security Council jointly hosted a tabletop exercise to examine cyber threats to critical infrastructure. More than 70 participants came from federal and state agencies, cybersecurity companies, energy and transportation operators, and crisis communications firms.

Divided into five teams, participants worked through a scenario simulating a cyberattack on the Baltimore power grid that had cascading effects on the regional transportation infrastructure.

The exercise's three moves – in which stakeholders **detected, responded to, and recovered from the cyberattack** – were structured around phases in the NIST Cybersecurity Framework.



Key Insights:

- Unclear lines of authority in a multi-jurisdictional crisis complicate decision-making.
- Government and infrastructure operators must maintain public confidence, in large part through comprehensive and accurate communication.
- Existing emergency management protocols may help localities cope with infrastructure failures caused by cyberattack; for example, snow-day closure procedures could minimize the number of people seeking access to crippled transportation systems by encouraging people to stay home and telecommute.
- Government agencies are more interested in the nature and origin of a cyberattack than infrastructure operators, which focus on restoring critical services.
- Existing public-private coordinating mechanisms – such as state intelligence fusion centers and sector-specific information sharing and analysis centers (ISACs) – can be used to share information and coordinate decision making by government and industry.

Preliminary Recommendations Include the Need For:

1. Further training and exercises to improve incident response;
2. Clear roles, responsibilities, and protocols for responding to cyberattacks;
3. Agreed-upon and exercised procedures for communicating and making decisions in a crisis that affects multiple state and local jurisdictions;
4. Decision making processes that ensure all affected parties have clear, centralized leadership advised by capable experts;
5. Widely understood and practiced procedures for operating critical infrastructure manually in case of power outages; and
6. Incentives for government and industry to share all relevant information in a crisis without fear of political or financial repercussions.

In the coming months, INSA will draft and disseminate a white paper that identifies cyber threats and infrastructure vulnerabilities, assesses relevant policies and crisis response procedures, and recommends steps to strengthen public-private partnerships and enhance infrastructure resiliency.

Thanks to INSA Members for Their Support

VENCORE Raytheon ICF S&A Spadaro & Associates

ABOUT INSA

The Intelligence and National Security Alliance's mission is to foster dialogue between public and private elements of the national security sector. INSA approaches this mission through a variety of means, including by organizing conferences, symposia, exercises, and other discussions. INSA also convenes government and industry experts in nine policy councils that address topics ranging from security clearance reform and insider threats to acquisition management and intelligence law.