National Cybersecurity & Communications Integration Center (NCCIC)

Homeland Security

NCCIC Overview

NCCIC Overview

- The National Cybersecurity and Communications Integration Center (NCCIC), a division of DHS' National Programs and Protection Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C), operates at the intersection of government, private sector, and international network defense and communications communities by:
  - Applying unique analytic perspectives
  - Ensuring shared situational awareness
  - Orchestrating synchronized response, mitigation and recovery efforts while protecting the Constitutional and privacy rights of Americans in both cybersecurity and communications domains.

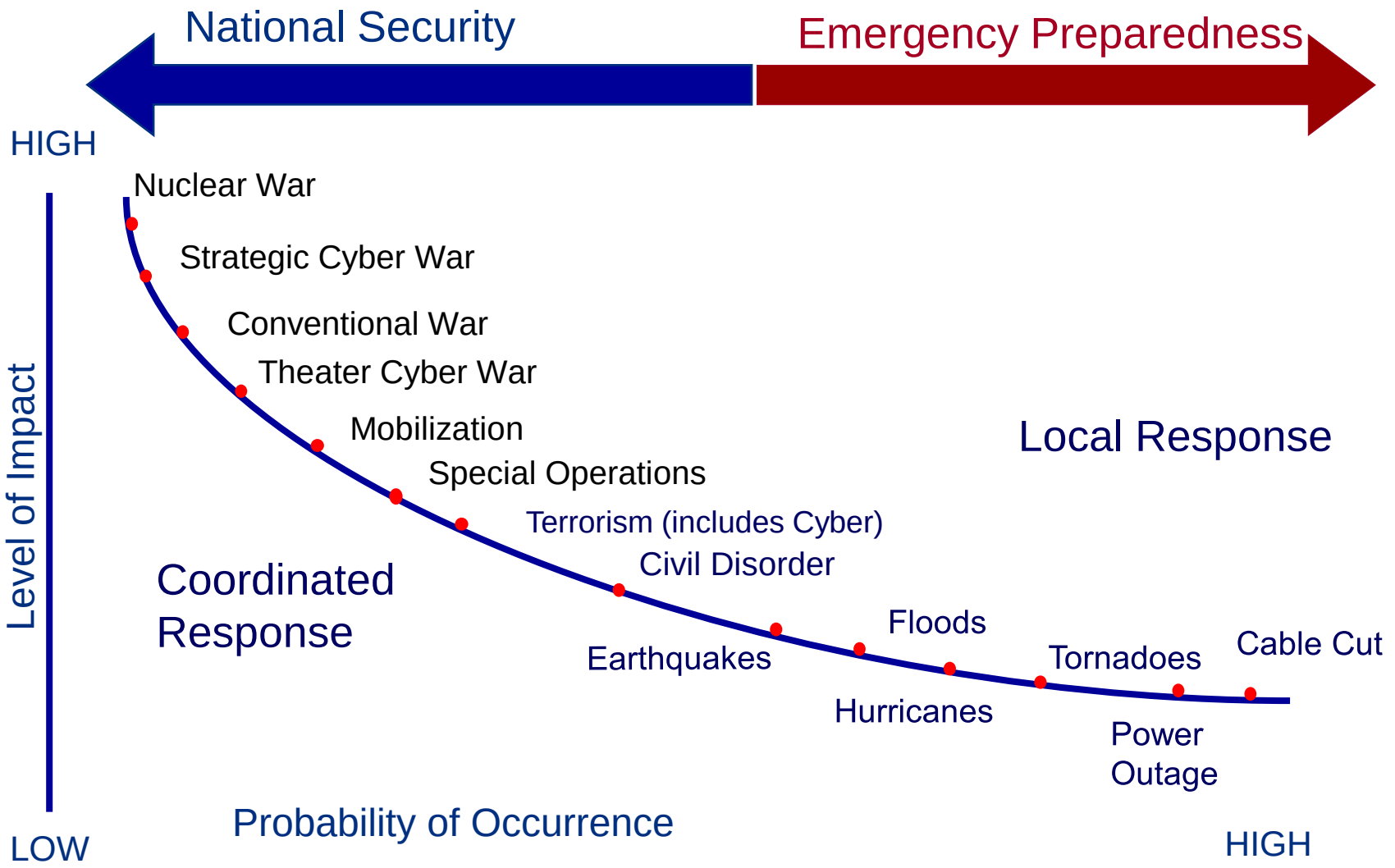
Four Components of the NCCIC

- **US-CERT**
- **ICS-CERT**
- **NCC**
- **O & I**

Homeland Security

Comm ISAC Industry Partners

Scope of Operations



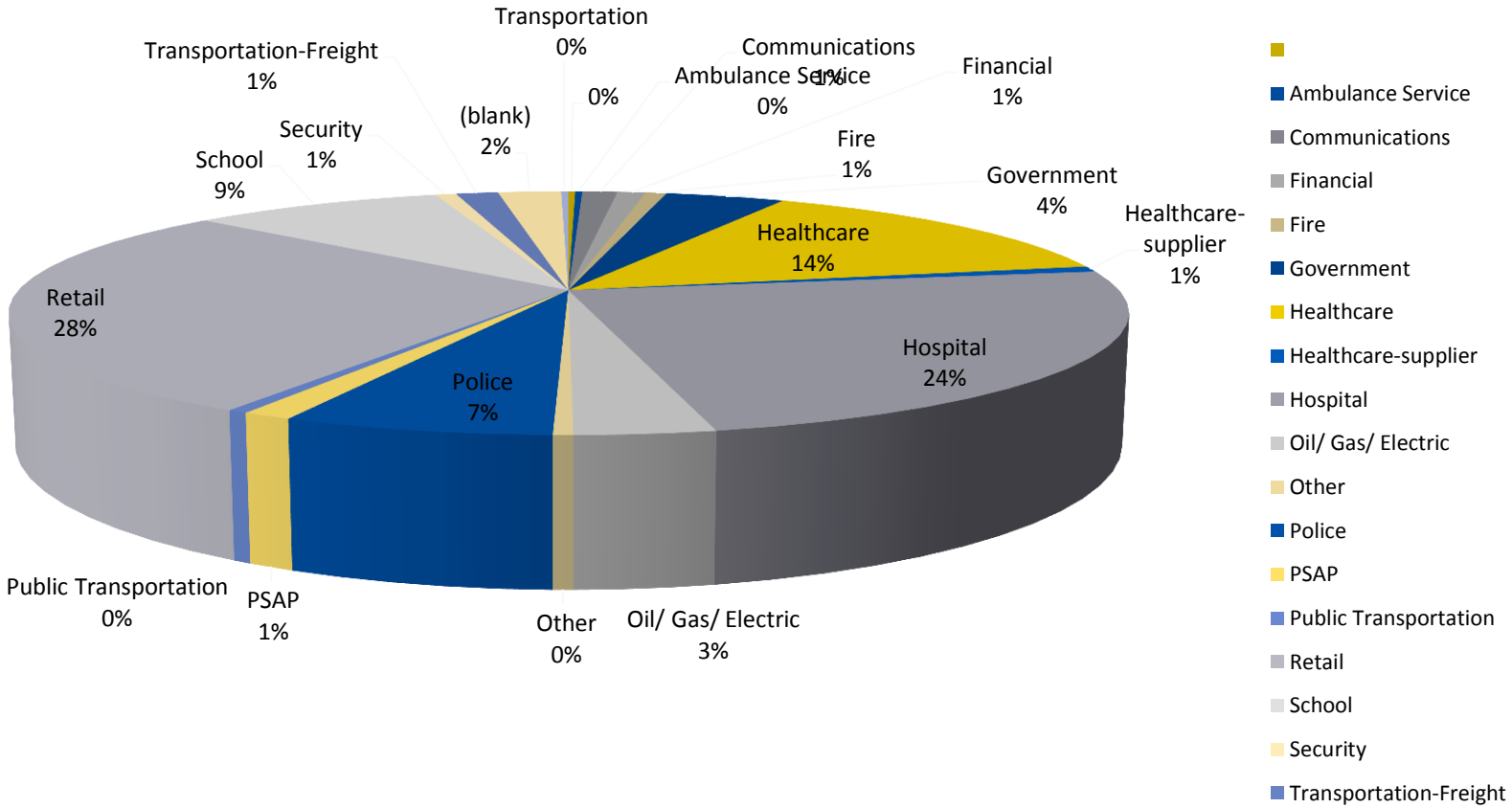
Homeland Security

Current Public Safety Issues

- Telephonic Denial of Service Attacks (TDoS)
- Spectrum Interference
- Disaster Communications Coordination (ESF-2)
  - Traditional ESF-2 Issues
  - Cyber attacks on public safety communications
  - Coordination of technical recovery resources in the event of a cyber attack with disaster level effects
- Migration to Next Generation 911
  - Cyber vulnerabilities and network defense leveraging NCCIC partnerships and capabilities
  - Coordinating protection of the .Gov Domain and sharing signatures and processes with public safety

Homeland Security

TDoS- Criminal Acts by Sector



Homeland Security

Jamming Spectrum

- There have been numerous reports of signal jamming devices employed to facilitate criminal activity and disrupt public safety operations
- Small handheld multi-frequency jammers capable of jamming Global Positioning Systems (GPS) and wireless communications including two-way radio communications
- Cost to purchase under $1000; some as little as $200
- Disrupts communications and/or GPS from 15 to 75 feet
- Concern of power boosting using off the shelf tools
- Local law enforcement typically does not have laws or capability to detect, identify or mitigate if they are confronted with jammers
- FCC & USDOJ have enforcement authority

Homeland Security

NCCIC Capabilities- TDoS & Jamming

- Develop Best Practices in coordination with public safety officials, telcom service providers, APCO & NENA on reporting, enforcement, legislative, and contingency ops, including Federal and International Law Enforcement coordination with DHS, FBI, FCC, FTC, DOS with UK & Indian investigators
- Coordination with key stakeholders
  - Emergency/First responders
  - Telecommunications Providers
  - Government Policy Community
  - Federal Emergency Communications Community
- Coordinate DHS/National Program Protection Directorate resources
  - Protective Security Advisors (PSAs)
  - Homeland Threat Reduction Analysis Center (HITRAC)
- Identify vulnerabilities to Cyber Attacks, TDoS Events and RF jamming
- Coordinating Cyber Center resources- MS ISAC

Homeland Security

Multi-State Information Sharing Analysis Center (MS-ISAC)

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24x7 Cyber Security Operations Center (SOC) provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.

MS-ISAC

MULTI-STATE
Information Sharing & Analysis Center

CENTER FOR
INTERNET SECURITY

Homeland
Security

Multi-State Information Sharing Analysis Center (MS-ISAC)

- MS-ISAC is only a phone call away to assist you with your Incident Response needs by providing you with the following capabilities:
- Malware Analysis
- Computer Forensics
- Network Forensics
- Incident Response
- Onsite Assistance
- Intelligence Coordination and Analysis

Homeland Security

Multi-State Information Sharing Analysis Center (MS-ISAC)

As these call centers move to a more data-centric model (Next Generation 911, VOIP) PSAPs are going to be increasingly susceptible to attack, as any other data network. MS-ISAC can help PSAPs with incident response and provide services, such as net flow monitoring.

MS-ISAC can assist with any Cyber attacks, such as intrusion, malware or DDoS. Currently MS ISAC has supported PSAPs, as information is shared through Cyber SOC notices for the IT personnel, CERT services, etc., pushed to our distribution lists and published on the MS ISAC Websites

MS-ISAC

MULTI-STATE
Information Sharing & Analysis Center

CENTER FOR
INTERNET SECURITY

Homeland
Security

Multi-State Information Sharing Analysis Center (MS-ISAC)

- Membership in the MS ISAC is free to qualified organizations
- If you would like to leverage the MS-ISAC for any of the above capabilities, please contact our 7x24 Security Operation Center by calling 1.866.787.4722 or emailing soc@msisac.org

MS-ISAC
MULTI-STATE
Information Sharing & Analysis Center
CENTER FOR INTERNET SECURITY
Homeland Security

Homeland Security