The Role of Intelligence and Information Sharing in Cyber

Mike Steinmetz
Former State Cybersecurity Officer: State of Rhode Island
President, Digital Executive Ltd.
Director & General Partner, College Hill Ventures

February 5, 2020; 3:00 PM
Brown University: Carmichael Auditorium,
85 Waterman St
Dr. John Savage, CSCI 1800 Cybersecurity

Objectives

- Provide an exposition of:
  - The cyber information and intelligence sharing environment
  - Organizations involved
  - Issues those organizations address
- Introduce you to some of the enablers, restrictions and challenges
- Reinforce through role-play

Role-Play Scenario for Today's Purposes

Rhode Island will host the World Games in 2025.
Cybersecurity is a major concern.

- You are asked to become a member of a cybersecurity coordination cell supporting the 2025 Games
- You are not sure what a cybersecurity coordination cell does; you attend anyway because it sounds interesting
- You arrive and notice there are many different people in the room.
- You think to yourself, "who are all these people and what do they do?"

Role-Play Scenario, Basic Questions

- What (who) exactly is the US Intelligence Community and why are they involved in this meeting?
  - By what authority are they allowed to act
  - What is their role in cybersecurity information sharing for the World Games
- Why are representatives of the Law Enforcement community here?
  - Regarding the FBI, by what authority are they allowed to act and support the effort?
    - What is their role in cybersecurity information sharing?
  - Regarding the State Police; same questions
- There are RI National Guard personnel attending the meeting. Why?
- Private sector leaders are present (President's and CEOs of electric, gas, water, communications). Why?
- There is a rumor that the Governor will attend. What authority does she have over the people and organizations in the room?
- Before you can sneak out a person in a military uniform approaches and says he/she are a Brown alum. The Governor arrives and the meeting begins. You're stuck.

Lets Freeze the Room

Who, What and By What Authority?

Organizations, US Title Code, Other Authorizing Documents, Authorities, Limitations

U.S. Intelligence Community

Who are they and what role do they play?

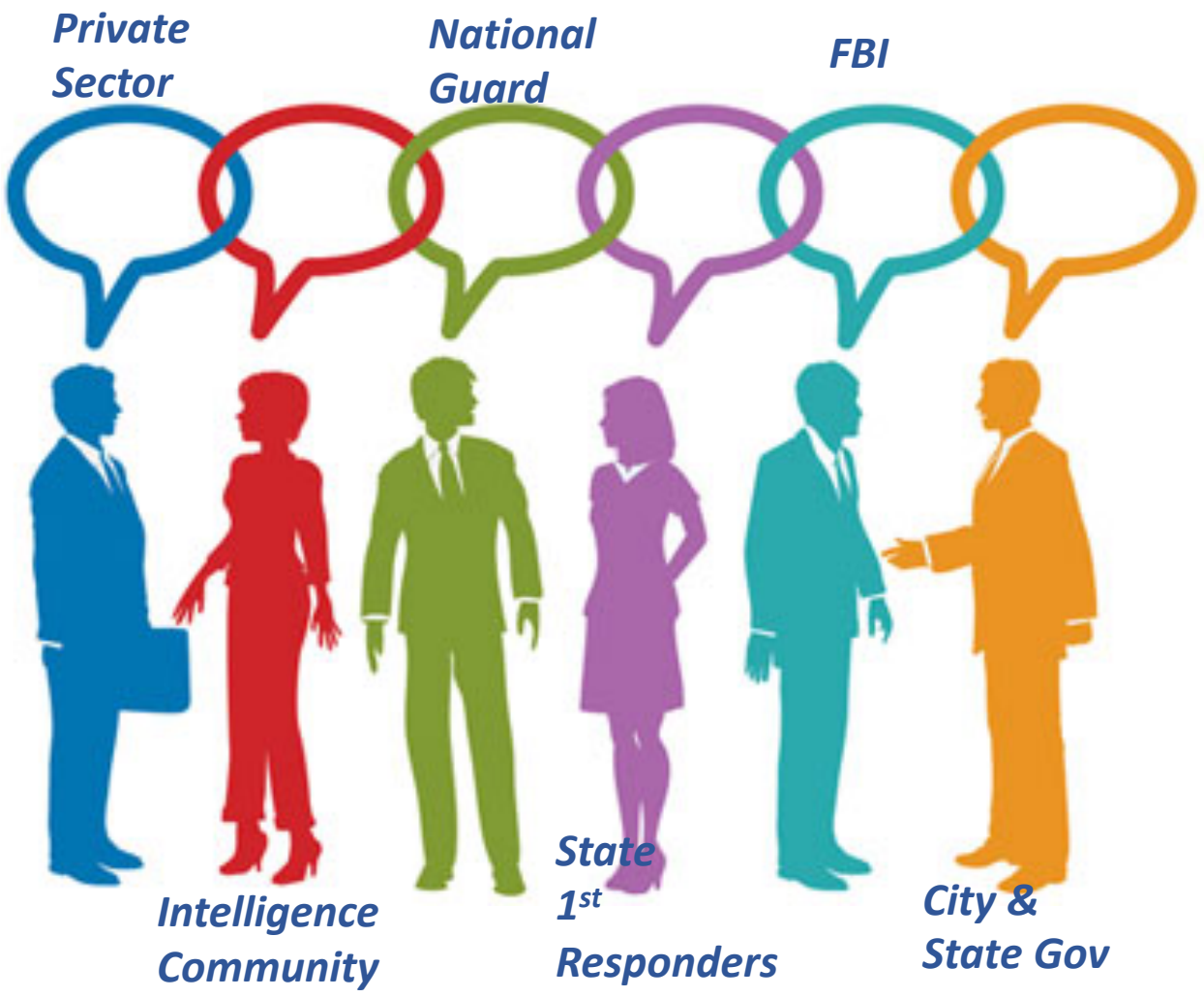
- 17 Agencies *(Elements)*
- Post 2004…17 Agencies + Office of the Director of National Intelligence

Others in the room with you

- National Guard (Air and Army assets)
- Rhode Island State Police
  - Computer Crimes (ICAC)
  - Joint Cyber Task Force (JCTF)
  - Fusion Center
  - Myriad other
- Academia
- Private Sector
- Trade Organizations
- CODEL representatives

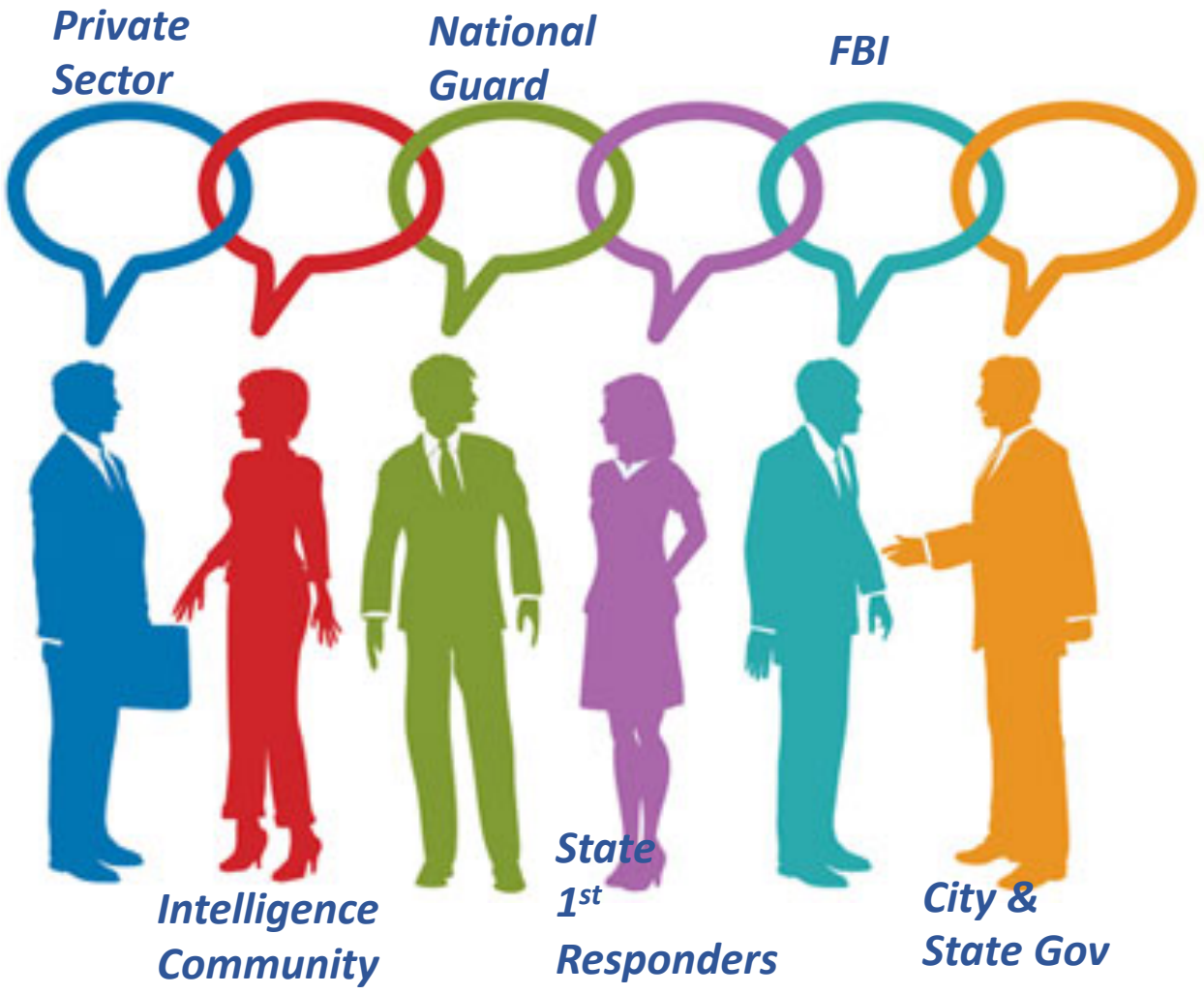
Authorities: U.S. Code, Executive Orders, Presidential Policy Directives, State Law, International Law, tweets etc. *Top-level list*

- Intelligence Community: Title 50 U.S. Code Responsibilities and authorities of the Director of National Intelligence
- Intelligence Community: Executive Order 12333 Timely, accurate, and insightful information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents
- Department of Defense: Title 10 U.S. Code provides the legal basis for the United States Department of Defense. However, special consideration is given to the National Guard and the US Coast Guard
- FBI: Title 28, U.S. Code, Section 533, Title 18 U.S. Code, Executive Order 12333; Title 50 U.S.C, Intelligence Reform and Terrorism Prevention Act of 2004. etc.



Authorities: …cont

- Private Sector: Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, Evaluate and mature the public-private partnership
- Private Sector: Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing. Create Information Sharing and Analysis Organizations (ISAOs) to promote better cybersecurity information sharing between the private sector and government, and enhance collaboration and information sharing amongst the private sector



Limitations on Civil Use of the Military

- Posse Comitatus Act
  - No use of the military in law enforcement role…except for US Coast Guard, and National Guard
- Some (not all) Exclusions and limitations to Posse Comitatus
  - Army and Air National Guard units and state defense forces while under the authority of the governor of a state.
  - Federal armed forces used in accordance to the Insurrection Act
  - The Attorney General may request that the Secretary of Defense provide emergency assistance for threats involving the release of nuclear materials
  - Enforcement of federal law at the discretion of the President of the United States (1957 Little Rock Central High School)

The National Guard

	STATE ACTIVE DUTY (SAD)	TITLE 32	TITLE 10
COMMAND AND CONTROL	Governor	Governor	President
LOCATION OF DUTY	Usually within the State, may be in other states (EMAC)	US	Worldwide
FUNDING	State	Federal	Federal
MISSION TYPES	In accordance with State law(riot control, emergencies)	Training and/or other federally authorized missions	Overseas Training and other missions as assigned
MILITARY DISCIPLINE	State Military Code/State Law	State Military Code/State Law	UCMJ/Federal Law
SUPPORT TO LAW ENFORCEMENT	Yes, within authority extended by state law	Yes, within authority extended by state law	As limited by Federal Law, Posse Comitatus Act
INDEMNITY FOR ACCIDENTS	State	Federal	Federal

Courtesy of the Adjutant General, State of Rhode Island

Other Topics Participants Discuss

- Import & Export
  - US Department of State Restrictions
    - International Trafficking in Arms Regulations (ITAR)
  - US Department of Commerce Restrictions
    - Export Administration Regulations (EAR)
- Federal government & other classifications commonly encountered
  - Unclassified but restricted use
    - For Official Use Only (FOUO)
  - Law Enforcement Sensitive (LES)
  - Confidential (C)
  - Secret (S)
  - Top Secret (TS)
  - No Foreign Dissemination (NOFORN)

Exhausted? Don’t Give Up! Homeland Security Can Help

Cybersecurity and Infrastructure Agency (CISA), Fusion Centers, ISACs & ISAOs

- DHS supports federal, private sector, and State Local Tribal Territorial (SLTT) customers by:
  - Serving as a hub for in *information sharing via State Fusion Centers ISACs and ISAOs*
    - Automated indicator sharing
    - Collaboration in the NCCIC
    - Alerts, warnings, and bulletins
  - Assisting with and coordinating significant incident responses
    - Onsite and remote incident response assistance
    - Exercises

Sharing Enablers to Remember

- Recent activity has been undertaken to allow for better intelligence and information sharing to take place
  - The National Infrastructure Protection Plan (NIPP) and Presidential Policy Directive (PPD) 21 identified sector specific critical infrastructure (Latest is Election Systems)
  - There are sector specific agencies that work with their sectors of the critical infrastructure (i.e., DHS for IT and Communications)
  - Some **Information Sharing and Analysis Centers** (ISACs) and **Information Sharing and Analysis Organizations** (ISAOs) are maturing operations and analysis based on information sharing
  - Legislation for information sharing: roles and responsibilities, liability relief, cybersecurity purposes only
  - Presidential Policy Directive (PPD) 41 – clarity on government roles and private sector expectations for government

Sharing Barriers to Keep in Mind

- Government barriers:
  - Classification (sources and methods)
  - Roles and responsibilities of government agencies
  - Conflicts between end-states:
    - Law enforcement
    - National security
    - Mitigation
  - Unclear authorities
  - Import Export
- Private Sector barriers:
  - Classification – ability to receive, the right personnel, etc
  - Perception of dealing with the government and some specific agencies
  - Liability
  - Multiple breech notification laws
  - Purpose for which the information received or provided is used

OK Unfreeze the Room

Lets Share Information!

Remembering of course all that other stuff I just said

Lots of Talk in the Room about Intelligence
What *exactly* is Intelligence

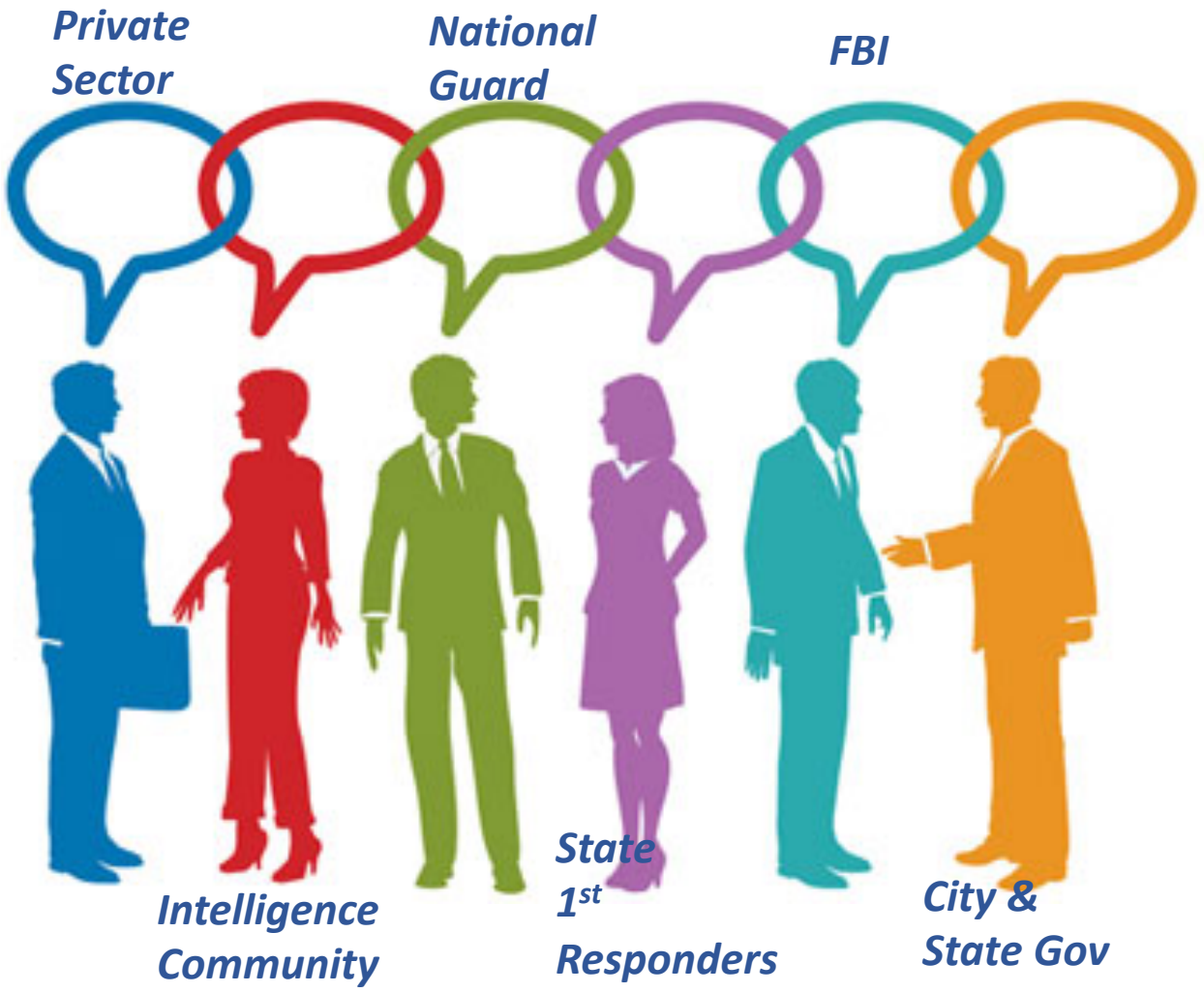
"Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs. Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analyzed responds to the needs of policy makers. All intelligence is information; not all information is intelligence."

Lowenthal, Mark M.. Intelligence: From Secrets to Policy (p. 2). SAGE Publications. Kindle Edition.

- Four Primary Activities
  - Collection
  - Analysis
  - Covert Action
  - Counterintelligence
- Six Steps of the Intelligence Cycle
  - Planning
  - Collection
  - Processing
  - Analysis
  - Dissemination
  - Evaluation
- Intelligence as **process**
- Intelligence as **product**
- Intelligence as **organization**

Participants raise the following cybersecurity-related concerns

- Protection of Basic Services (Electric/Gas/Water)
- Protection of Emergency Services (Hospitals/RX/Fire/LE)
- Protection of Venue Services (Tickets etc)
- Protection of information services (TV/Internet/cell)
- Emergency communications (special communications)
- Counterterrorism (social media, big data analysis, Human Intelligence)
- Transportation (natural/man made disaster)
- International issues (rogue state)



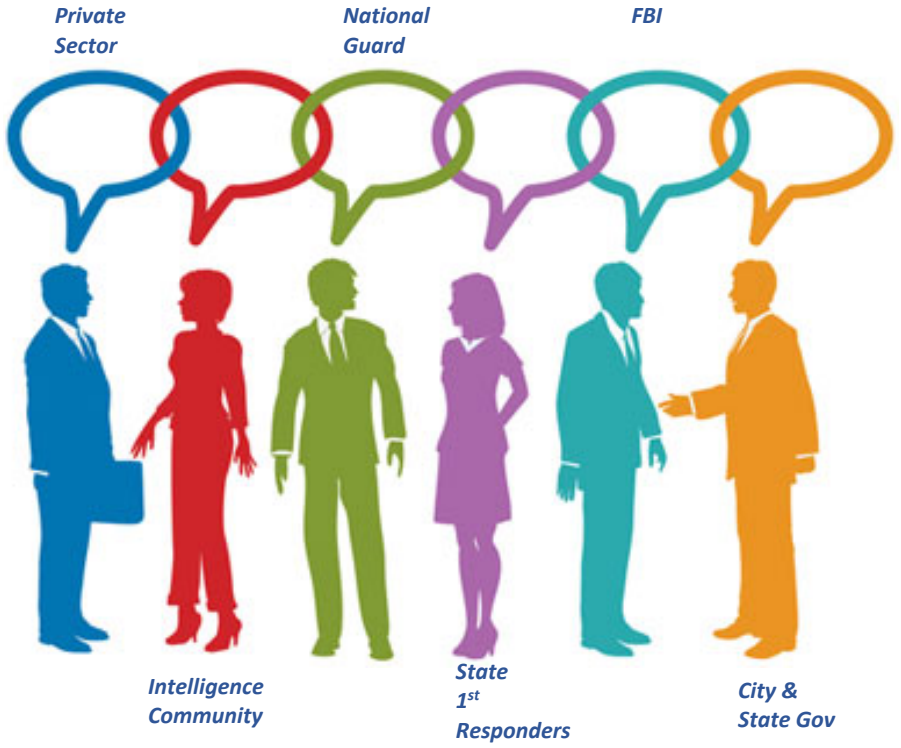
OK! Now Lets go!

Rhode Island will host the World Games in 2025.
Cybersecurity is a major concern. Let's begin collaborating

Address a Cybersecurity Problem

Think through; be ready to role play

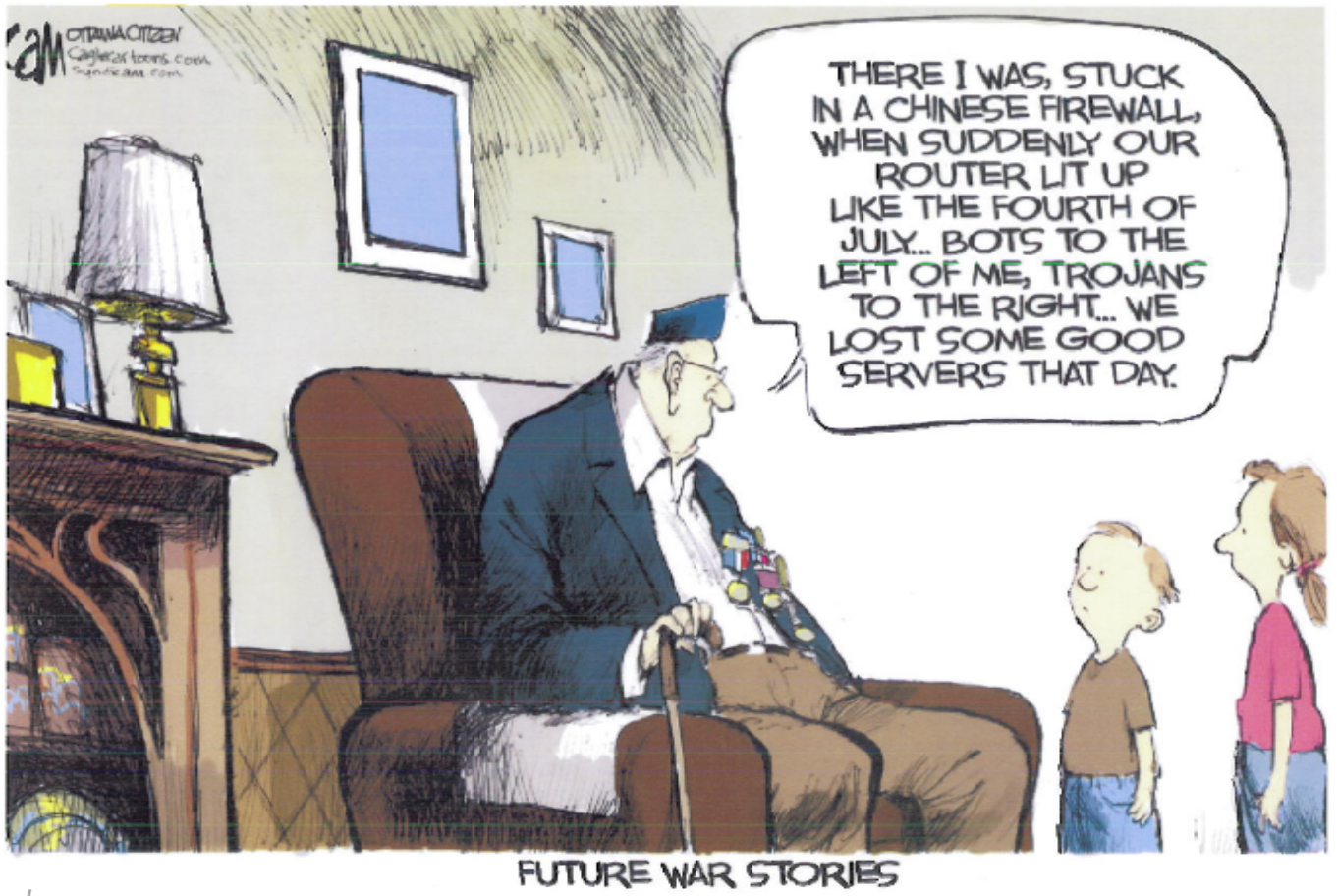
- Protection of Basic Services (Electric/Gas/Water)
- Protection of Emergency Services (Hospitals/RX/Fire/LE)
- Protection of Venue Services (Tickets etc)
- Protection of information services (TV/Internet/cell)
- Emergency communications (special communications)
- Counterterrorism (social media, big data analysis, Human Intelligence [HUMINT])
- Transportation (natural/man made disaster)
- International issues (rogue state)



Think About

What Information Do you Need? Who (or what organization) might have that information?
Do you need intelligence? Who might have the intelligence you need?
What restrictions might "respondents" impose on the information or intelligence they provide?

Questions?



Mike Steinmetz
Former State Cybersecurity Officer: State of Rhode Island
President, Digital Executive Ltd.
Director & General Partner, College Hill Ventures

Some lite Reading Before Bedtime

- 18 U.S. Code § 1385 - Use of Army and Air Force as posse comitatus. (n.d.). Retrieved January 13, 2020, from https://www.law.cornell.edu/uscode/text/18/1385.
- EMAC. (2019). Emergency Management and National Guard Duties/Authorities. Retrieved January 13, 2020, from https://www.emacweb.org/index.php/national-guard.
- Executive Order 13636: Improving Critical Infrastructure ... (n.d.). Retrieved January 13, 2020, from https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.
- Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing. (2019, May 28). Retrieved January 13, 2020, from https://www.dhs.gov/publication/executive-order-13691-promoting-private-sector-cybersecurity-information-sharing.
- IRTPA. (2004). Retrieved January 13, 2020, from https://www.dni.gov/files/NCTC/documents/RelatedContent_documents/Intelligence_Reform_Act.pdf.
- Obama Administration Releases Long Awaited New E.O. 12333 Rules on Sharing of Raw Signals Intelligence Information Within IC. (2019, October 31). Retrieved from https://www.lawfareblog.com/obama-administration-releases-long-awaited-new-eo-12333-rules-sharing-raw-signals-intelligence.
- ODNI. (2019). How the IC Works. Retrieved January 13, 2020, from https://www.intelligence.gov/how-the-ic-works#.
- Presidential Policy Directive 21 Implementation. (n.d.). Retrieved January 13, 2020, from https://www.dhs.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper-2015-508.pdf.