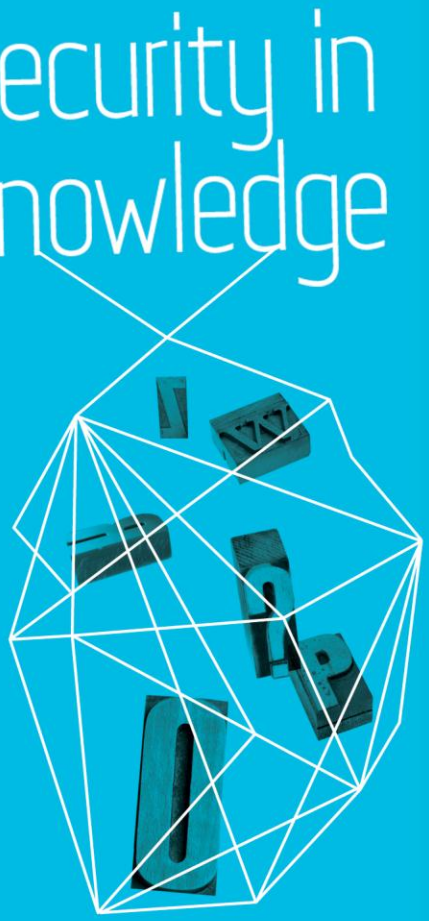
Do We Have the Authority? Legal Issues in Protecting Government Networks



Moderator:

Gib Sorebo
SAIC

Panelists:

Kevin Gronberg
U.S. House of Representatives

Elliot Oxman
U.S. Department of Energy

Roland Trope
Trope and Schramm LLP

John Gregory
Ministry of Attorney General
Ontario, Canada

Session ID: LAW-T18

Session Classification: Intermediate

Legal Limitations on Defenses

- Electronic Communications Privacy Act / Wiretap Act
- Two-party consent statutes
- Third-party services providers
- Civilian vs. law enforcement vs. military vs. intelligence activities
- General privacy restrictions (U.S. federal, states, international)
- Computer Fraud and Abuse Act

Defense Scenarios – Government Employees and Unauthorized Actors

- Insider threat
  - Employee exfiltrating sensitive information
  - Committing financial fraud
- Denial of service attacks
  - At what level can agency block an attack?
  - What is needed to shut down or disconnect the offending node?
- Other investigations of waste, fraud, and abuse
  - What is needed to search employee work-provided computer?
  - What about personally owned mobile device with agency data and applications on it?
  - What about services provided by third-party cloud provider that agency pays for?

Defense Scenarios – Citizens

- Insider threat (authorized citizen system users)
  - Exceeding authorization
  - Committing financial fraud
- Citizen interactions
  - Ability to monitor communications ("on the wire")
  - Ability to search databases and stored communications for evidence of illegal activities
  - Private communications with agency employees
- Cross-border and foreign national interactions
  - Whose laws apply?
  - How was data obtained and under what conditions?

Legal Reform – What's Needed?

- Monitoring clarifications
  - Who, what, when, where, why, and how
- When and how to "hack back"
- Information sharing
  - Privacy considerations
  - Classified data
  - Timeliness of information
  - Actionable with little or no interpretation

Takeaways

- Don't assume that if it's on your network you can monitor it and act on the information obtained
- Ensure legal counsel has reviewed security operations plan, including monitoring and incident response
- Define policies that include and notify all stakeholders as explicitly as possible
  - Employees
  - Contractors
  - Service providers
  - Citizens
  - Foreign nationals

Questions?