The “Internet of Things”

and the

National Infrastructure!

2018: A Cyber Space Odyssey

presented by the

National Security Forum of Reno, NV

with

Jerry Morris

Agenda

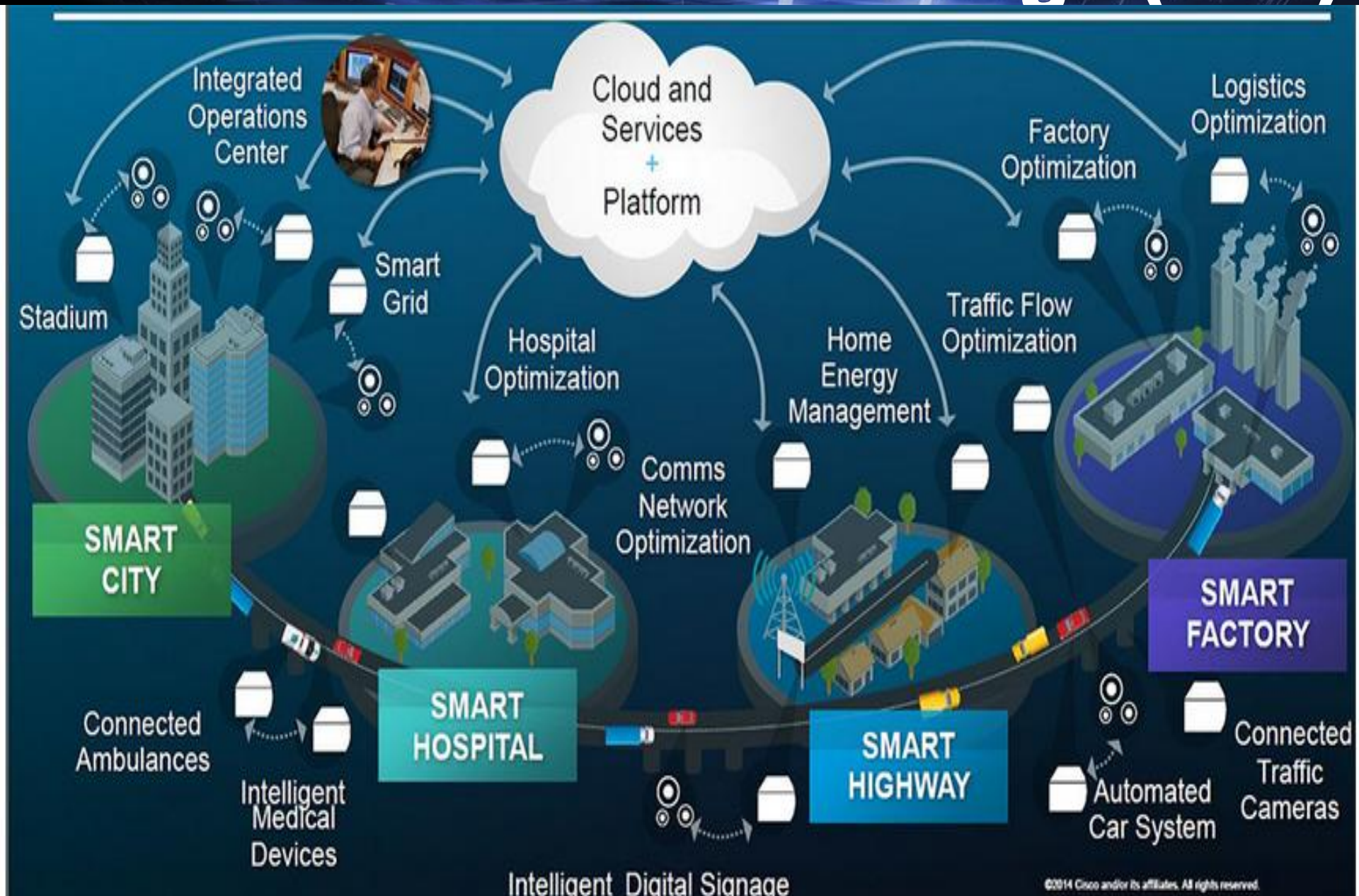
- BLUF: No Silver Bullet
- What is IoT / IIoT / ICS / SCADA
- Types and Methods of IIoT / ICS Attack
- Pathway into the ICS
- IIoT / ICS Targets
- Recent IoT / ICS Attacks
- Economic Impact
- IIoT / ICS Forensics
- Modernize Cyber Laws
- Moving Forward
- Questions

Bottom Line Up Front

- The Internet of Things (IoT) is the fastest growing digital capability, application or function
- Thousands of Industrial cyber-attacks daily with new forms of Malware continuously released
- 5th Domain of Warfare and requires minimal cost
- U.S. infrastructure is privately owned and poorly defended
- Tremendous damage and confusion with no silver bullet, need multi-layered strategy

Internet of Things (IoT)

Industrial Internet of Things (IIoT)



Industrial Control Systems (ICS)

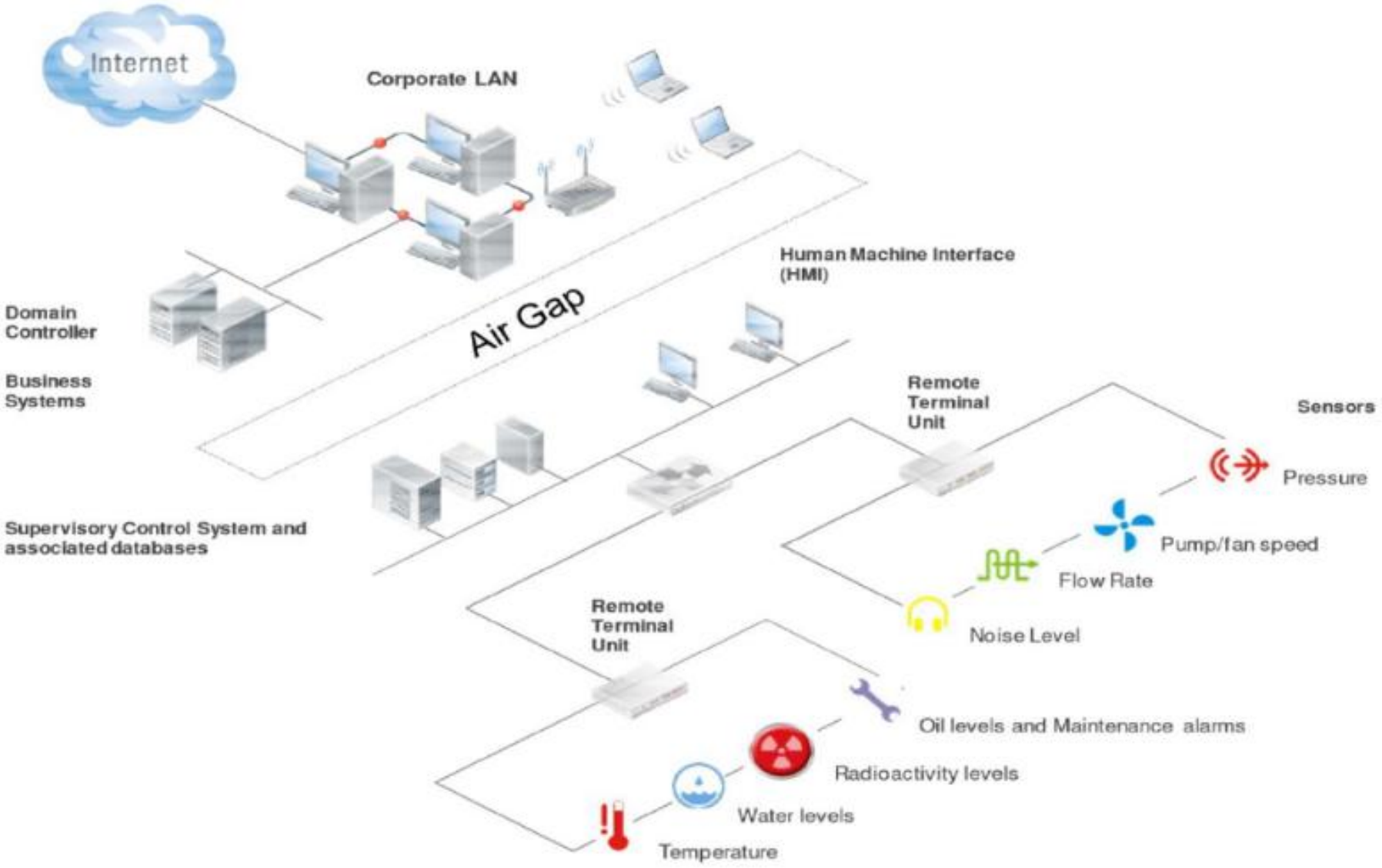
- **Defined:** The integration of administrative and operational hardware and software with network connectivity in order to support industrial applications or functions within the critical infrastructure.

  - **Supervisory Control and Data Acquisition (SCADA)**
  - Distributed Control Systems (DCS)
  - Industrial Automation and Control Systems (IACS)
  - Programmable Logic Controllers (PLC)
  - Programmable Automation Controllers (PAC)
  - Remote Terminal Units (RTUs)
  - Control Servers
  - Intelligent Electronic Devices (IEDs)
  - Sensors

Industrial Control Systems (ICS)

- Legacy Systems with extensive patching
- ICS components have limited computing processor and memory resources
- ICS components have multiple access points and not designed with operational security
- Limited number of IT / OT professionals

SCADA System



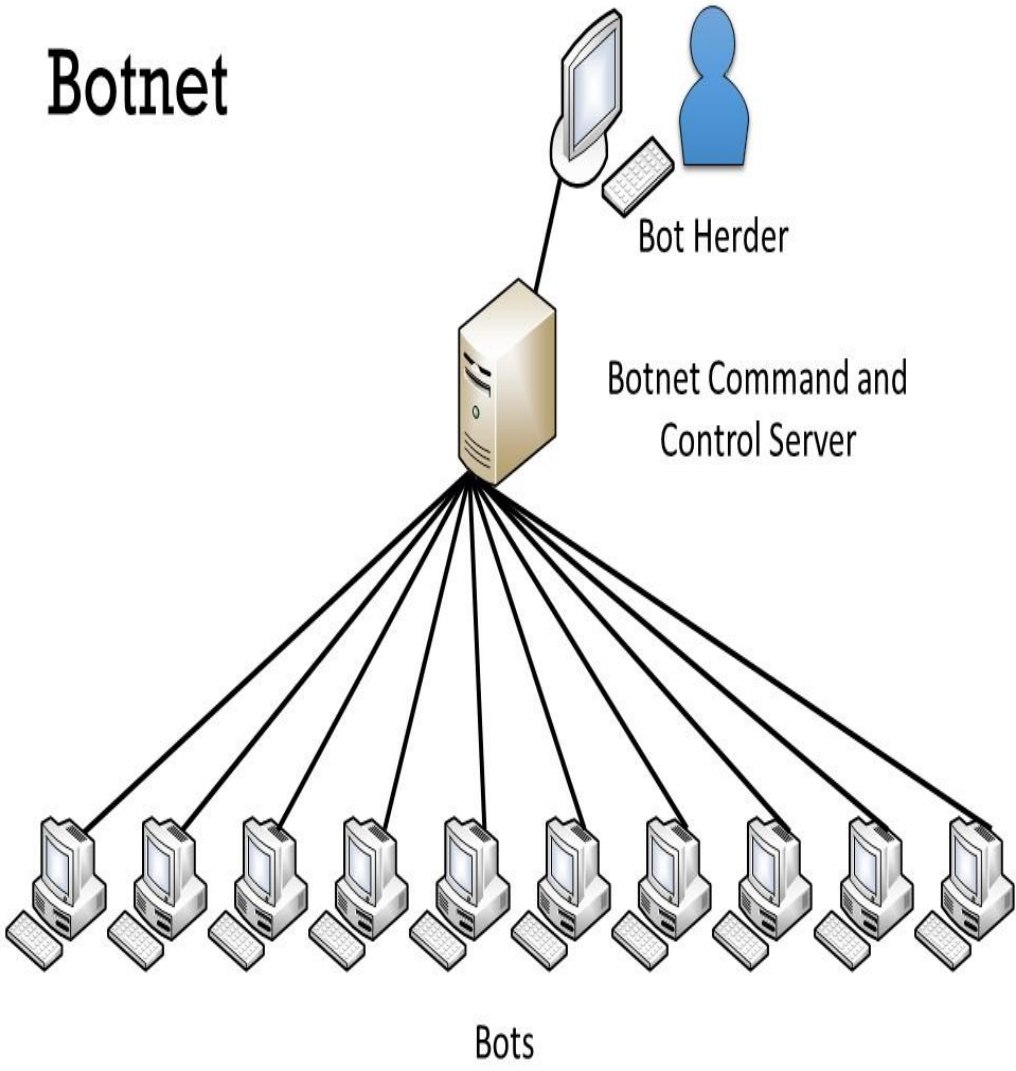
IIoT / ICS - Threat

- External: Most Likely
  - Financial gain, political or military objective
  - State-sponsored, competitors or hacktivists
- Insider Threats: Most Dangerous
  - Malicious / Intentional
  - Unintentional / Accidental /Consequential
- Hybrid: External with Insider Access:
- Increasing in sophistication, continue to evolve, improving tactics, techniques and procedures faster than security teams can keep up.

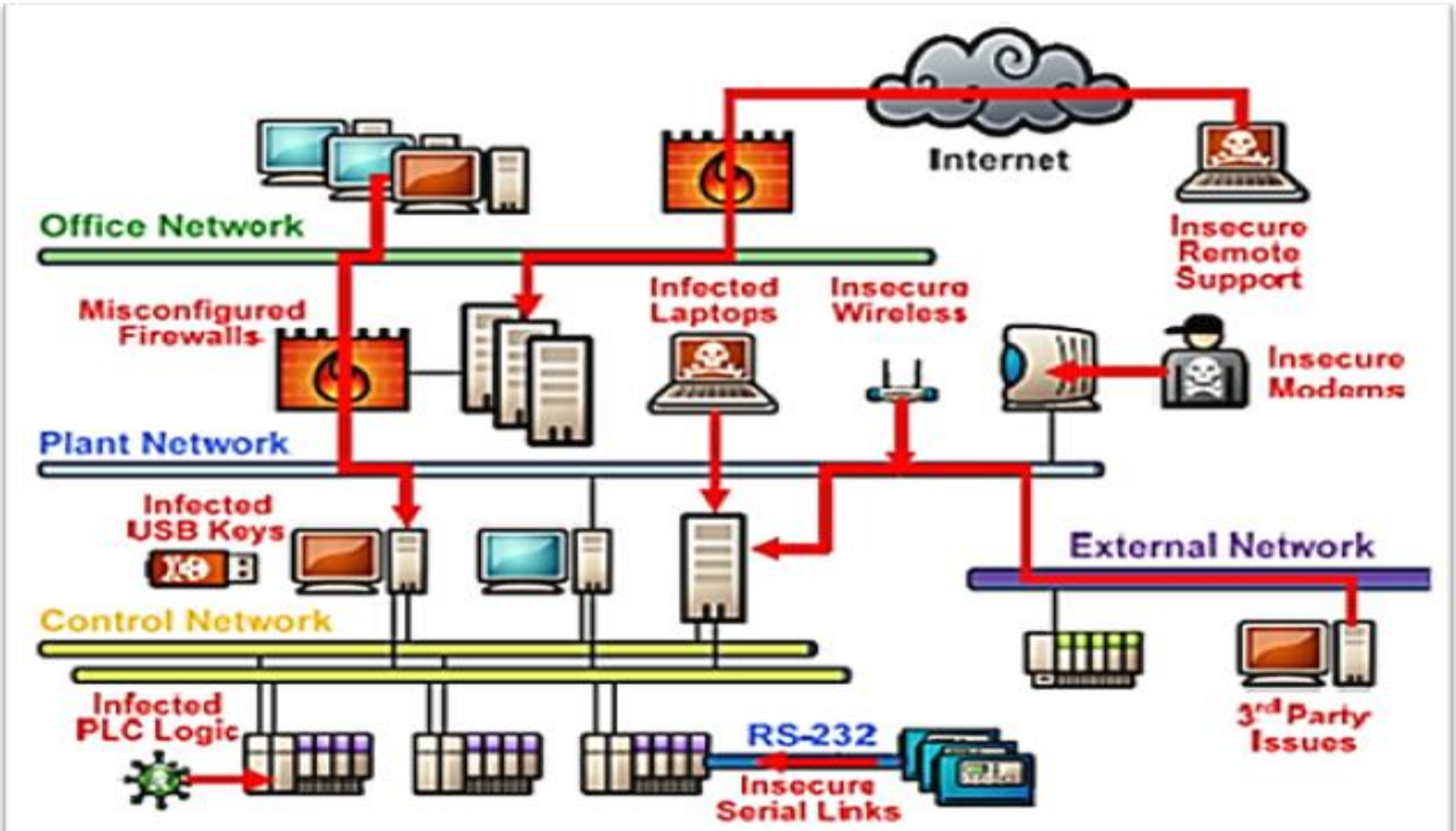
Types of IoT / ICS - Attack

- Phishing
- DOS / DDOS
- Ransomware
- Worm / Virus
- Trojan
- Brute Force
- Miscellaneous

Methods of IoT / ICS - Attack



Pathway into the Control System



Possible Pathways into the Control System

IIoT / ICS Targets

- Infrastructure: Nuclear, Electrical, Solar, Wind, Gas, Water, Sewer, Communications, Dams, etc.
- Industrial / Manufacturing
- Transportation Assets / Traffic Controls
- Medical / Healthcare
- Government / Military
- Education / Research

2007 Auraura Cyber-Test

Recent Infrastructure Attacks

- **2007: Russia / Estonia - City wide DDOS - Sabotage**
- **2010: U.S. / Iran – Centrifuge - Stuxnet Worm- Sabotage**
  - 2013: Iran / U.S - Natanz - Theft from US Banks in Retaliation
- **2013: Iran / U.S. - Rye Brook, NY Dam Attack - Cellular Modem**
- **2015: Russia / Ukraine - Elec Grid - Black Energy APT**
- **2015: Russia / French - Water Shed - Triton Virus**
- **2016: Russia / U.S. - Elec Grid, Vermont - Grizzly-Steppe Tool**
- **2016: Russia / U.S - Election Machines - "NotPetya" Ransomware**
- **2017: Russia / U.S. - Wolf Creek Nuclear Plant, Kansas - Phishing**
- **2018: Russia / U.S. - Boeing in-flight fires - "Wanna Cry Virus"**

Economic Impact

- Theft of Proprietary Info and PII
- Critical Infrastructure Damage / Loss of all utilities
- Failure of Life Support Systems with all business and banks closed
- Long term recovery / Commodities rationed
- Chaos / Confusion / Injury / Death

IIoT / ICS - Forensics

- Limited Capabilities for IIoT / ICS
- Identify / Collect / Preserve / Analysis / Report
- Response timeline 48 hours
- Zone Approach / Eco-System Approach
- Opportunity / Means / Motive
- Do’s and Don’ts
- Organization Training / Exercises / Recovery Drills

Modernize Cyber-Laws

- Domestic Criminal Law
- International Law
- Law of War: “Jus ad Bellum” “Use of Force”
- Rules of Engagement Electronic / Magnetic / Kinetic

Moving Forward

- Conduct multi-layered strategy
- Increase funding
- Implement IT / OT cyber education programs
- Replace legacy systems and components
- Develop IoT-forensics to reverse engineer attacks
- Modernize cyber-laws to prosecute using forensics
- Future research and development


Questions