TENTH ANNUAL LEADERSHIP EVENT

# CYBER SECURITY SUMMIT

*Security solutions through collaboration.™*

## THE RIPPLE EFFECT

The Cascading Impacts of Cyber Security

**OCTOBER 26–28, 2020**

cybersecuritysummit.org

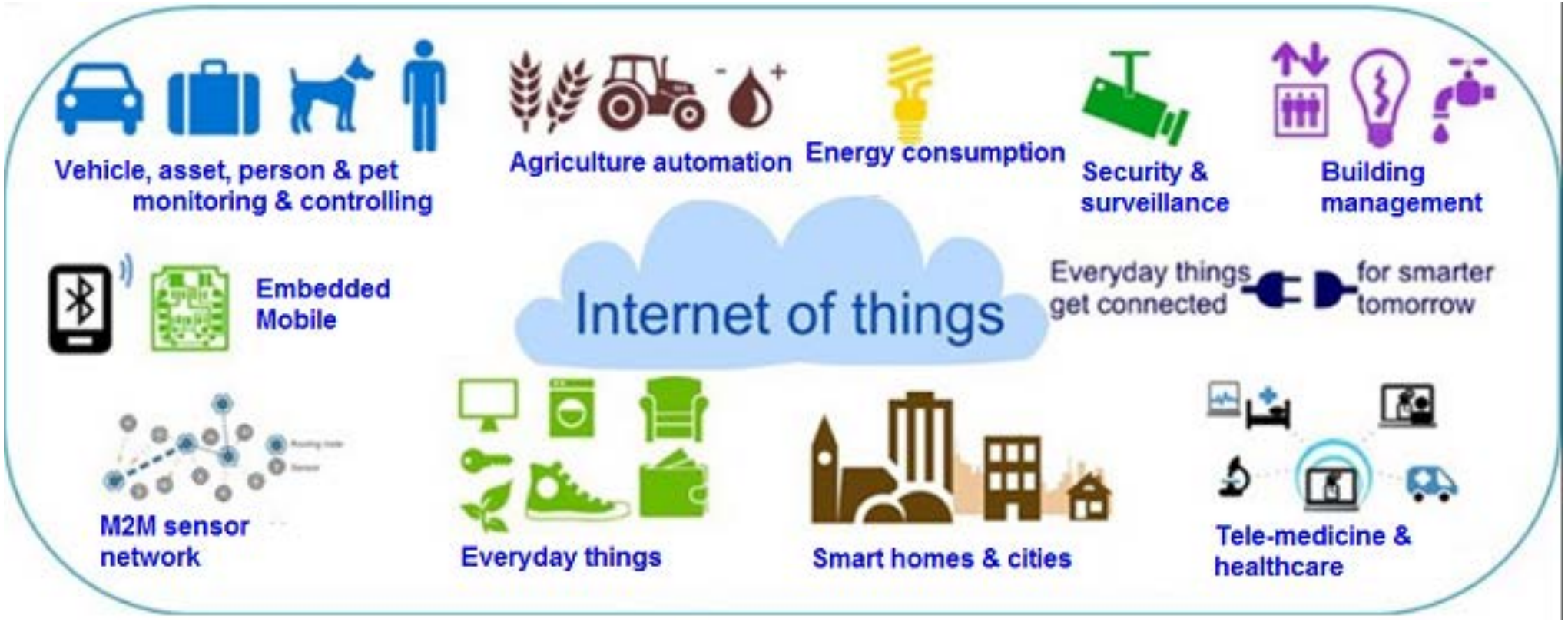
10 YEAR ANNIVERSARY


Norwich University Applied Research Institutes

# THANK YOU

Phil Susmann, President
Tom Muehleisen, Director of Cyber Operations

# Internet of Things - IoT




https://Tcefnc.org/iot-club 10/21/20

# National Critical Functions

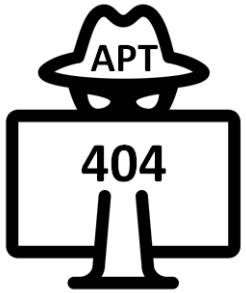
- The functions so vital their disruption would have a debilitating effect on society

- Many of these functions are provided through IoT!

## National Critical Functions

| CONNECT | DISTRIBUTE | MANAGE | SUPPLY |
|---|---|---|---|
| - Operate Core Network<br>- Provide Cable Access Network Services<br>- Provide Internet Based Content, Information, and Communication Services<br>- Provide Internet Routing, Access, and Connection Services<br>- Provide Positioning, Navigation, and Timing Services<br>- Provide Radio Broadcast Access Network Services<br>- Provide Satellite Access Network Services<br>- Provide Wireless Access Network Services<br>- Provide Wireline Access Network Services | - Distribute Electricity<br>- Maintain Supply Chains<br>- Transmit Electricity<br>- Transport Cargo and Passengers by Air<br>- Transport Cargo and Passengers by Rail<br>- Transport Cargo and Passengers by Road<br>- Transport Cargo and Passengers by Vessel<br>- Transport Materials by Pipeline<br>- Transport Passengers by Mass Transit | - Conduct Elections<br>- Develop and Maintain Public Works and Services<br>- Educate and Train<br>- Enforce Law<br>- Maintain Access to Medical Records<br>- Manage Hazardous Materials<br>- Manage Wastewater<br>- Operate Government<br>- Perform Cyber Incident Management Capabilities<br>- Prepare for and Manage Emergencies<br>- Preserve Constitutional Rights<br>- Protect Sensitive Information<br>- Provide and Maintain Infrastructure<br>- Provide Capital Markets and Investment Activities<br>- Provide Consumer and Commercial Banking Services<br>- Provide Funding and Liquidity Services<br>- Provide Identity Management and Associated Trust Support Services<br>- Provide Insurance Services<br>- Provide Medical Care<br>- Provide Payment, Clearing, and Settlement Services<br>- Provide Public Safety<br>- Provide Wholesale Funding<br>- Store Fuel and Maintain Reserves<br>- Support Community Health | - Exploration and Extraction Of Fuels<br>- Fuel Refining and Processing Fuels<br>- Generate Electricity<br>- Manufacture Equipment<br>- Produce and Provide Agricultural Products and Services<br>- Produce and Provide Human and Animal Food Products and Services<br>- Produce Chemicals<br>- Provide Metals and Materials<br>- Provide Housing<br>- Provide Information Technology Products and Services<br>- Provide Materiel and Operational Support to Defense<br>- Research and Development<br>- Supply Water |

# IOT Failures (or another name)




- Botnets and Deadbolts and Cameras… OH, MY!
  - 2019 Top Ten
    1. Continued Mirai Botnet Growth
    2. Smart Deadbolts
    3. ‘Systemic’ Privacy Flaws
    4. Privacy Concerns For IoT Hotel Devices
    5. All Things Ring
    6. Malware Bricks Thousands of IoT Devices
    7. Smart Toys
    8. IoT Smartwatches
    9. Smart Speakers
    10. 2 Million IoT Devices Vulnerable to Complete Takeover

*Source: Threatpost - https://threatpost.com/*

## MITRE ATT&CK for ICS

| Initial Access | Execution | Persistence | Evasion | Discovery | Lateral Movement | Collection | Command and Control | Inhibit Response Function | Impair Process Control | Impact |
|---|---|---|---|---|---|---|---|---|---|---|
| Data Historian Compromise | Change Program State | Hooking | Exploitation for Evasion | Control Device Identification | Default Credentials | Automated Collection | Commonly Used Port | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Drive-by Compromise | Command-Line Interface | Module Firmware | Indicator Removal on Host | I/O Module Discovery | Exploitation of Remote Services | Data from Information Repositories | Connection Proxy | Alarm Suppression | Change Program State | Denial of Control |
| Engineering Workstation Compromise | Execution through API | Program Download | Masquerading | Network Connection Enumeration | External Remote Services | Detect Operating Mode | Standard Application Layer Protocol | Block Command Message | Masquerading | Denial of View |
| Exploit Public-Facing Application | Graphical User Interface | Project File Infection | Rogue Master Device | Network Service Scanning | Program Organization Units | Detect Program State | | Block Reporting Message | Modify Control Logic | Loss of Availability |
| External Remote Services | Man in the Middle | System Firmware | Rootkit | Network Sniffing | Remote File Copy | I/O Image | | Block Serial COM | Modify Parameter | Loss of Control |
| Internet Accessible Device | Program Organization Units | Valid Accounts | Spoof Reporting Message | Remote System Discovery | Valid Accounts | Location Identification | | Data Destruction | Module Firmware | Loss of Productivity and Revenue |
| Replication Through Removable Media | Project File Infection | | Utilize/Change Operating Mode | Serial Connection Enumeration | | Monitor Process State | | Denial of Service | Program Download | Loss of Safety |
| Spearphishing Attachment | Scripting | | | | | Point & Tag Identification | | Device Restart/Shutdown | Rogue Master Device | Loss of View |
| Supply Chain Compromise | User Execution | | | | | Program Upload | | Manipulate I/O Image | Service Stop | Manipulation of Control |
| Wireless Compromise | | | | | | Role Identification | | Modify Alarm Settings | Spoof Reporting Message | Manipulation of View |
| | | | | | | Screen Capture | | Modify Control Logic | Unauthorized Command Message | Theft of Operational Information |
| | | | | | | | | Program Download | | |
| | | | | | | | | Rootkit | | |
| | | | | | | | | System Firmware | | |
| | | | | | | | | Utilize/Change Operating Mode | | |

Source: https://collaborate.mitre.org/attackics/index.php/Main_Page

# Understanding (your) Vulnerabilities

- *"If you know the enemy and **know yourself**, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."* — Sun Tzu, The Art of War

- CSC Top 20 #1. Inventory and Control of Hardware Assets

- Pen Tests are #20… *think about it.*

# Organizational Resilience

- Asset Inventory for all functions and devices
- Determine dependencies and requirements
- Wargame Impact and Vulnerability
- Prepare for Compromise-Destruction
- Practice Response
- Capture Lessons and Improve Resilience

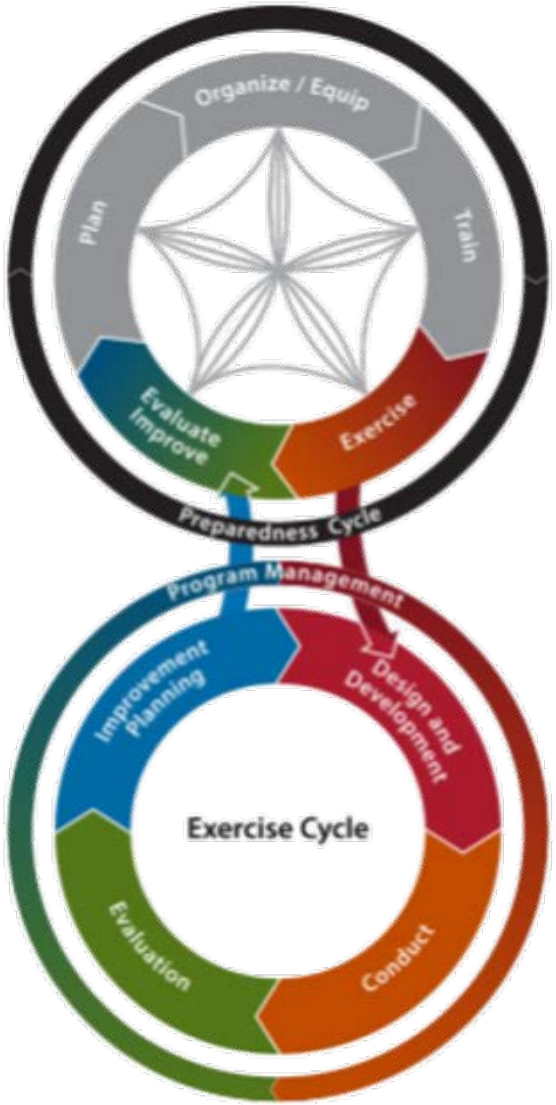




**Figure 2.1: Integrated Preparedness and Exercise Cycle**

**Source: FEMA HSEEP**

# Future Considerations

- CISA
  - NCFs: https://www.cisa.gov/national-critical-functions
- NIST
  - IoT: https://www.nist.gov/topics/internet-things-iot
- CIS
  - CSC Top 20: https://www.cisecurity.org/controls/cis-controls-list/

# Questions/Discussion


**Phil Susmann, President**
**Tom Muehleisen, Director of Cyber Operations**