New Approaches to Protecting Critical Infrastructure from Cyber Attack

Linton Wells II
Centre of Excellence for National Security (CENS)
Distinguished Visitor Program (DVP) Lecture
September 2, 2016
Topics

• Types of Critical Infrastructures

• Observations from black hat and DEF CON

• Malicious Cyberspace Activities vs. Infrastructure Controls

• Characteristics of Smart Cities, Smart Nation Singapore

• Cyberspace Concerns in Smart City environments

• New Cybersecurity Approaches

• Opportunities and Risks for Singapore
### Critical Infrastructures

Responsibilities typically assigned to ministries/departments

In US, DHS’s National Protection & Programs Directorate's (NPPD) Office of Infrastructure Protection (IP) leads coordinated national efforts to build resilience

<table>
<thead>
<tr>
<th>Singapore Sectors (10)</th>
<th>US Sectors (16)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economics</td>
<td>Commercial Facilities</td>
</tr>
<tr>
<td>Information</td>
<td>Communications</td>
</tr>
<tr>
<td>Security &amp; Emergency</td>
<td>Critical Manufacturing</td>
</tr>
<tr>
<td></td>
<td>Dams</td>
</tr>
<tr>
<td></td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td></td>
<td>Emergency Services</td>
</tr>
<tr>
<td>Energy</td>
<td>Energy</td>
</tr>
<tr>
<td>Banking and Finance</td>
<td>Financial Services</td>
</tr>
<tr>
<td>Government</td>
<td>Government Facilities</td>
</tr>
<tr>
<td>Health Care</td>
<td>Healthcare &amp; Public Health</td>
</tr>
<tr>
<td></td>
<td>Information Technology</td>
</tr>
<tr>
<td>Environment</td>
<td>Nuclear Reactors, Material, Waste</td>
</tr>
<tr>
<td>Transportation</td>
<td>Sector-Specific Agencies</td>
</tr>
<tr>
<td>Water</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td></td>
<td>Water &amp; Wastewater Systems</td>
</tr>
</tbody>
</table>
Interconnections

Superstorm Sandy example (2012)

- power, fuel and comms

- Some stations had fuel but no power to pump
- Some had power, but no fuel
- Decision-support systems didn’t integrate
- Comms often disrupted
Velocity of Tech Change

If a factor, e.g. computing power/unit cost, doubles every 18 mo, 5 yr increase is 900%, 10 yr 10,000%, by 2030 ~100,000%

Biotech even faster, robotics ubiquitous, nano poised breakout, energy impacts are global
- Think BRINE (bio-robo-info-nano-energy) + Additive Manufacturing
  Interactions complicate things
Linear projections CAN’T work
Planning and Engineering for Resilience

• Take **whole-of-society** approach:
  – Public-private, whole-of-government, transnational

• Address all dimensions: **Physical, Cyber, Human, Temporal**

• Consider scenarios (set in context)
  – Include threats, resources, tech change, political will, etc.—look ahead

• Analyze risk—consider:
  – Dependencies, including cross-sector vulnerabilities
  – Pathways to risk exposure (e.g. safety vs. security)
  – Cascading casualties
  – Overall risk across all dimensions

• Examine stakeholder perceptions
  – Including mental models

• Combine training, exercises, education and incentives to **change behavior**
  – Remember that **no lesson is ever learned until behavior changes**

• **ACT EARLY**
  – Designing in is ALMOST ALWAYS better than adding on afterwards
black hat/DEF CON 2016 Observations

• **No** reason for complacency about cybersecurity

• **Speed:** Reducing Time to Detect (TTD) of malware, remediate flaws faster, and aggressively update code

• **Infrastructure remains vulnerable,** complicated by exploding weaknesses in the Internet of Things (IoT)

• Software Defined Radios (SDR) and Software Defined Networks (SDN) can be secured, but
  – they require people who can integrate hardware and software fixes, and very skilled systems administrators

• DARPA’s **Cyber Grand Challenge** (CGC) offered something new with Artificial Intelligence & Machine Learning (but far off)
black hat briefs re Smart Grid/Industrial Security

• Drone Attacks on Industrial Wireless: A New front in Cyber Security [electronic attacks via drone]
• The Risk from Power Line Communications [G3 PLC sniffing]
• What’s the DFIRrence for ICS? [Digital Forensics and Incident Response] for embedded devices
• Advanced CAN Injection Techniques for Vehicle Networks
• Understanding HL7 2.x Standards, Pen Testing, and Defending HL7 3.x Messages [health care messaging]
• The Tao of Hardware, the Te of Implants [Hardware hacking]
• PLC Blaster: A Worm Living Solely in the PLC [Siemens Simatic]

black hat briefings are at: https://www.blackhat.com/us-16/briefings.html
Many of the DEF CON briefings are at: https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/

DEF CON Infrastructure-Related Events

• **Villages**
  – Car Hacking
  – Hardware Hacking
  – IoT
  – Lockpick
  – Social Engineering
  – Wireless (including Software-Define Radios-SDR)
  – Packet Hacking

• **Workshops**
  – Pentesting Industrial Control Systems (ICS) 101
  – Applied Physical Attacks on Embedded Systems

• **Presentations**
  – How to Remote Control an Airliner: Security Flaws in Avionics
  – Picking Bluetooth Low Energy Locks from a Quarter Mile Away
  – Hacker-Machine Interfaces: The State of the Union for SCADA HMI Vulnerabilities
  – All Your Solar Panels Are Belong to Me
  – Hacking Hotel Keys and Point-of-Sale Systems
  – Attacking Base Stations—An Odyssey Through a Telco’s Network [via eNodeB]
  – Network Attacks Against Physical Security Systems
  – Can You Trust Autonomous Vehicles: Contactless Attacks Against Sensors of Self-Driving Vehicles
Malicious Cyberspace Actions

- Deny
- Disrupt
- Degrade
- Destroy
- Deceive

- Combine with Information Operations
- Combine with kinetic actions
Industrial Control Systems (ICS) & SCADA Systems (Supervisory Control and Data Acquisition)

ICS/SCADAs are ubiquitous, but HIGHLY insecure

- Most architectures not designed for security
- Multiple entry and attack paths
- Default settings weak—vulnerable on reboot
- Often old, hard to fix
- IoT (Cloud of Everything) will dramatically increase “attack surface”
Types of Attacks Against ICS/SCADA

• Human Machine Interface (HMI)—200+ vulnerabilities discovered
• Distributed Denial of Service (DDOS)
• Remote penetration
• Hardware/firmware modification
• Supply chain vulnerability
• Social engineering
• Cleared insider
• Targets
  – Pressure/temperature/voltage modification
  – Set point modification
  – Programmable Logic Controllers (PLCs)
• Examples: Hospital and production line modification
Internet of Things (IoT)

- Should be “Cloud of Everything”—human body becoming a platform, apps interact
- Growing attack surface
  - IHS projects 53 billion IoT devices by 2020, 3x 2013*
  - More than 300 kinds of IoT have been hacked
  - 26% of cyber attacks in Japan in 2015 targeted IoT devices
- Almost NO market demand for security
  - Functionality and speed-to-market dominate priorities
- Be careful not to build “Smart Nation” on a foundation of sand
  - Internet Engineering Task Force (IETF) began work on IoT in 2006—use them
- Educate people in cyber security
  - Lou Gerstner story
  - Singapore could do this better than most

*Japan News Aug 24, 2016, p. 1
Characteristics of Smart Cities

A smart city uses digital technologies or information and communication technologies (ICT) to

- enhance quality and performance of urban services
- reduce costs and resource consumption
- engage more effectively and actively with its citizens

Source: SmartCitiesCouncil

Cyberspace is a key part of Smart Cities
Projected Smart City ICT Revenue

Source: Andrew Brown, Strategy-Analytics

One estimate is $977 billion by 2022
Smart Nation Singapore

• Smart Nation Platform (SNP): Connect, Collect & Comprehend → Create
  – Above-Ground (AG) Boxes
  – Heterogenous Network (HetNet)

• Benefits
  – Citizens: Greater citizen-centric services, empowerment
  – Businesses: Enable innovation
  – Public agencies: Greater efficiency, stronger inter-agency cooperation

• Steps: Sensor Mapping, Smart Traffic, Smart Homes
Cyberspace Concerns in Smart City Environments

• Organizations, People, Processes, Technology

• Many stakeholders, level of collaboration

• Skill sets, agendas

• Governance, whole-of-society approaches

• Control tech, underlying tech, rate of change
Cyberspace Planes

- **Supervisory** – Often siloed/compartmentalized between sectors
- **Persona** - Relevant identities or accounts; do you know who to contact in other sectors?
- **Logical** - System compatibility; how do various networks and systems communicate?
- **Physical** - Redundancy; can connectivity be compromised?
- **Geographic** - Physical location can be important!

Also have Cross-Cutting Vulnerabilities among Infrastructures

From: Greg Conti, et. al., PEN Testing a City Briefing presented at black hat Aug 2015
Risks for Singapore

• Single impactful events
  – Disrupt services
  – Damage infrastructure
  – Injure people

• Persistent disruptions, e.g. rolling blackouts
  – Political pressure, job action

• Multi-domain campaign like RU is mounting against Ukraine
  – Undercut people’s confidence in government
  – Influence political actions
New Cybersecurity Approaches Opportunities for Singapore

• Boundary control points and segmented enclaves
• Cyber Secure Microgrids--SPIDERS
• Secure Codes/Components
• NRT anomaly detection and response
  – Hawaii Electric Company (HECO)
  – Supervisory Phasors
• Educated Population
• AI & ML and binaries
Opportunities for Singapore (1)
Boundary Control Points & Segmented Enclaves

Tesla security architecture shows there IS a secure alternative

Typical car today
- Mixes Infotainment LAN and vehicle control CAN (Controller Area Network)
- Multiple RF paths into LAN
- Hard to patch

Tesla
- Separates LAN & CAN
- Crypto-secure bridge
- Over-the-air fixes

Can Tesla-like “wrapper” be applied to traditional SCADA systems in Singapore’s systems?
Applications

• Wrapper for ICS/SCADA

• USN “Cyber Resiliency”
  – Boundary Control Points/
    Enclave Segregation
  – Design in Security
  – Multi-level training

• Japanese “protective wall” idea *
  IoT Devices | Protective Wall | Internet
  at Home     | (System)       |

Internal Affairs and Comms Ministry

* Japan News Aug 24, 2016, p. 1
Opportunities for Singapore (2)
Cyber Secure Microgrid--SPIDERS

SPIDERS
(Smart Power Infrastructure Demonstration for Energy Reliability and Security)

Cyber-secure microgrid architecture:
- smart grid technologies
- distributed and renewable generation
- energy storage

on military installations to enhance mission assurance

Phase 1: Single circuit demo of cyber-secure microgrid for waste water treatment
Phase 2: Multi-building demo
- Integrated large solar PV array and microgrid connected electric trucks

Phase 3: DoD’s first installation-wide microgrid

Next step is project transition, possibly to private sector
Opportunities for Singapore (3)
Use More Secure Codes/Components

Cybersecurity liability costs likely to rise

- Some project 25-30% of IT budgets will be for insurance in a few years
  - These funds not available for investment or innovation
  - Per Singtel, today’s cyber insurance market is under developed

- Singapore could set codes requiring more secure components, and focus on more secure interoperability

- Build on reputation for quality
  - Lower insurance costs and liability risk
  - Consider how “Smart Buildings” can contribute to security of “Smart Cities”
  - Perhaps as part of secure microgrids
Opportunities for Singapore (4)

Near-Real Time Anomaly Detection

• Supervisory Phasors
  – Collect data across grid

• Big Data Analytics
  – Near-Real Time (NRT) anomaly detection
  – Irrespective of source
  – Address problems directly

Linton Wells II, linwells@gmail.com, +1 202.436.6354
9/2/2016 final
Opportunities for Singapore (5)

Educated Population

• Teach on many levels
  – Executives/Commanders
  – Managers
  – Cyber

• Life-long learning

• Develop elite skills

Random vs Scale-Free Networks
(also describes distribution of hacker/defender skills)

Opportunities for Singapore (6)
Artificial Intelligence (AI) & Machine Learning (ML)

• DARPA’s Cyber Grand Challenge (CGC) offered something new:
  – Artificial Intelligence (AI), Machine Learning (ML), and Big Data Analytics, plus
  – Focus on security operations at the binary level and
  – “formal verification” of code, offer ways to
  – “imagine a future with some likelihood of cybersecurity”*

• Long term project, but it offers a way ahead
  – But ML algorithms also can be hacked

*DARPA Director Dr. Arati Prabhakar, at DEF CON Aug 5, 2016
Opportunities for Singapore (7)

Sept 14, 2015 US “Smart Cities” Initiative

- $160M in Federal research & leverage over 25 tech collaborations
- Help local communities reduce traffic congestion, foster economic growth, manage climate change impacts, improve service delivery

Four strategies

- Test beds for IoT apps & multi-sector collaborative models
- Collaborate with civic tech movement, inter-city collaboration
- Leverage existing Federal activity
- Pursue international collaboration

Singapore-related areas:

- $10M Cyber-Physical Systems Program, includes smart buildings
- $2.5M Global City Teams Challenge: integrate networks & physical
- $2.5M for research to improve interdependent infrastructures
- $3M from DoE to advance smart building technologies
Ways that Companies can Contribute

• Rethink Public-Private Partnerships for Smart Nation

• Commit to “Smarter & Greener” Construction
  • Smart buildings
  • Use reliable components
  • Energy management
  • Green energy

• All contribute to:
  • Enhanced quality and performance of urban services
  • Reduced costs and resource consumption

• Corporate Social Responsibility (CSR)
  • Smart City projects
Summary

• These are big issues

• Can’t be taken for granted

• The “smarter” the city, the bigger the “attack surface”
  – Consider “thin line” fallback

• But lots of opportunities
QUESTIONS?

linwells@gmail.com

Skype: linwells

U.S. cell +1 202.436.6354