Keeping Hackers Out of the Smart Grid

Webinar presented by IEEE Power and Energy Society and Industrial Application Society of Northern Virginia/Washington

27 January 2021

Presenter:
Ryan Davidson – rdavidson@mpr.com

www.mpr.com

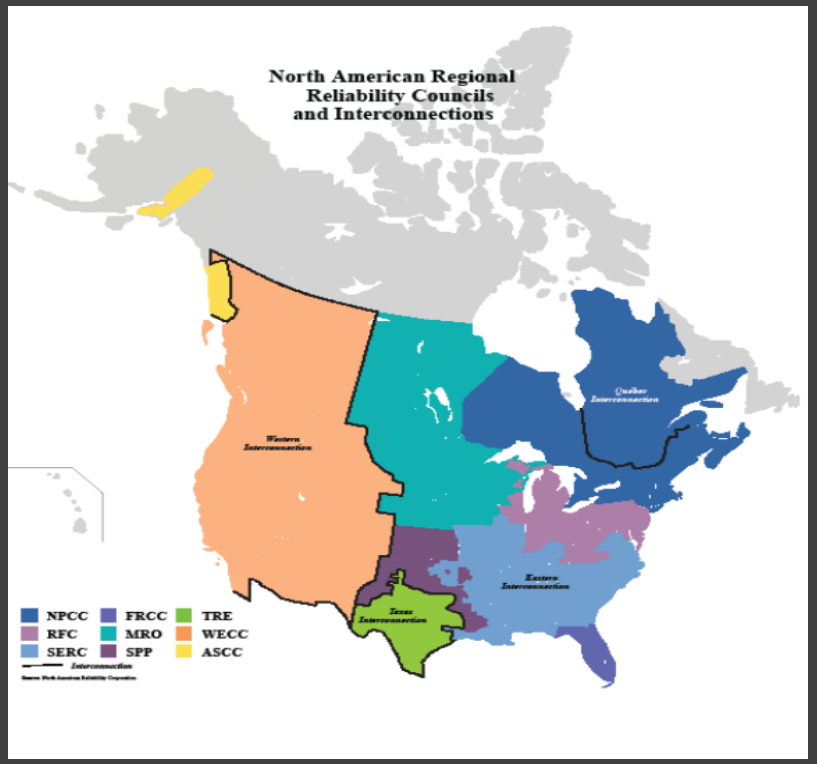
Speaker Overview

Ryan Davidson

- Electrical Engineer with MPR Associates
  - Industrial Control Systems and Cybersecurity
- Global Industrial Cyber Security Professional
- IEEE Member
  - Power and Energy Society member
  - Subgroup lead for technical recommendations for 1547.3 “Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems”
- Army Veteran (249th Engineering Battalion)

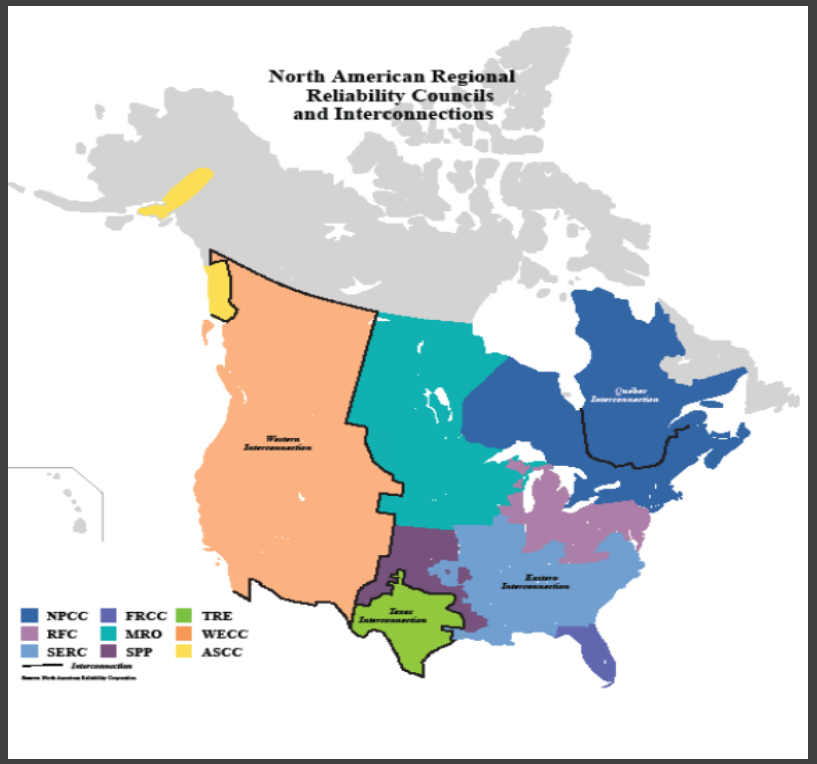
North American Bulk Electric System

- Large integrated system of generation, transmission and distribution, and loads
- Comprised of three large primary interconnections (Western, Eastern, Texas)
- Complex and dynamic system
- Tasked with providing safe and reliable power at all times



North American Bulk Electric System

- Large integrated system of generation, transmission and distribution, and loads
- Comprised of three large primary interconnections (Western, Eastern, Texas)
- Complex and dynamic system
- Tasked with providing safe and reliable power **at all times**



Impact of Power Outage

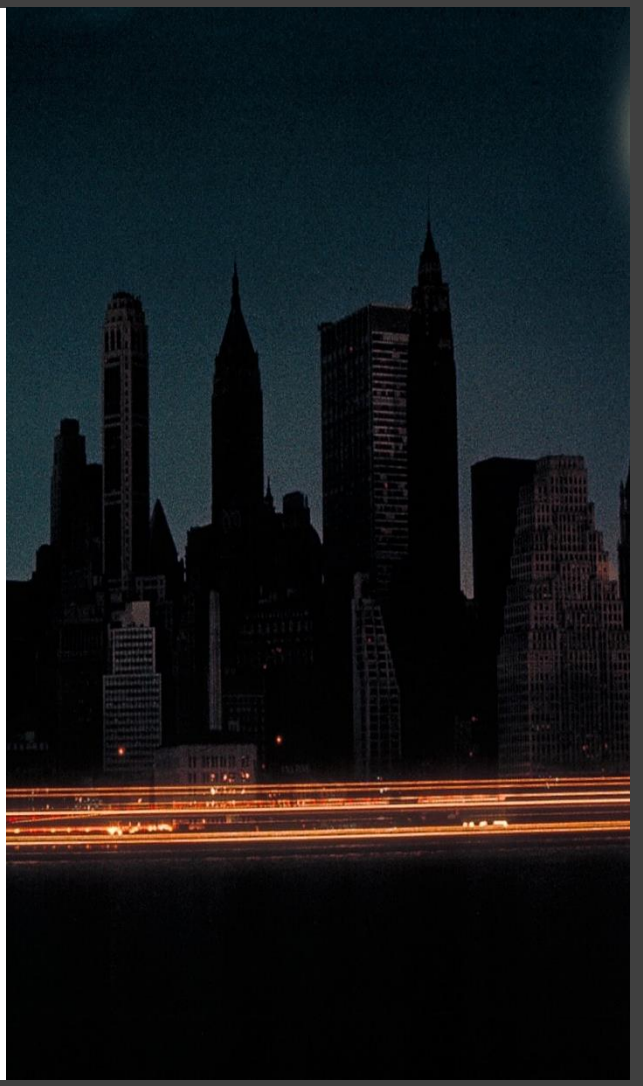
What happens when the Bulk Electric System (BES) fails to provide power?

- Communication networks are lost or overloaded
- Residential areas are without heating or cooling
- Businesses are forced to close
- Critical facilities must transition to back up power
    - Back up systems are often not well maintained and are prone to failure
- Potential for casualties including loss of life
- Safety concerns with loss of lighting and security systems
- Sanitation and public water concerns
- Costs can be in the billions

Impact of Power Outage

BES is historically very reliable although not perfect

- Northeast Blackout (1965)
  - *30 million customers for 13 hours*
  - Poor relay setting
  - Lack of voltage and current monitoring
- Northeast Blackout (2003)
  - *50+ Million customers*
  - Cost $4-$10 billion
  - Caused by software bug, poor vegetation maintenance, inadequate system planning, inadequate data monitoring, and inadequate contingency planning, validation and execution
- Derecho Blackout (2012)
  - *Over 4 Million customers for 7-10 days*
  - Caused by severe weather
  - Estimated $7.5 billion
- Puerto Rico and Hurricane Maria (2017)
  - *1.5 million customers*
  - Nearly 1 year to fully restore power



Can a cyber attack cause the same damage?

Ukraine Power Grid Attacks

- 2015 and 2016 first publicly known successful cyber attack on a power grid
- Phishing -> Active Directory compromised -> Disabled UPS for operators -> TDOS to cripple utility call center -> Took over workstations and opened breakers -> Overwrote remote access firmware -> Wiped operator workstations
- Including Industroyer (a.k.a. CrashOverride) and Black Energy 3 malware toolkits
- 30 substations were switched off resulted in loss of power for 1-6 hours for more than 225K customers.
- Loss of remote control of substation controllers for extended period and forced to operator manually for months

Saudi Aramco

Shamoon

- 2012 attack on business network
- 30K – 35K machines partially wiped or destroyed crippling the corporate network
- Initial access through phishing then further compromising several systems on the network
- Shamoon is wormable and overwrites the master boot record = bricked hard drive

Triton

- 2017 attack on Triconex Safety Instrumented System (SIS)
- Initially misdiagnosed even by the vendor as equipment failure
- Failed goal of causing physical harm with control of Distributed Control System (DCS) and SIS

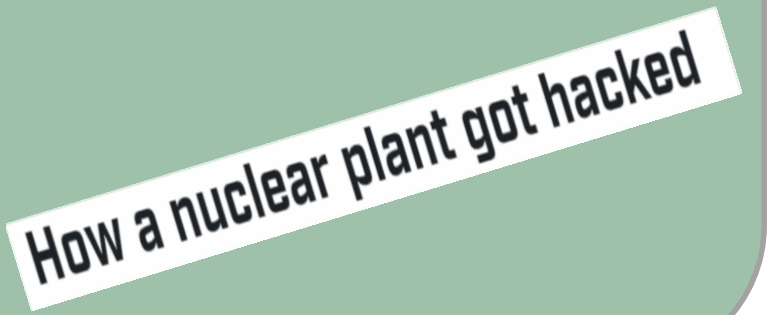
Can a cyber attack cause the same damage?

Stuxnet

- Natanz uranium enrichment facility in Iran
- Data exfiltration from third-party supplier -> developed custom malware with several zero-days -> malware delivered via removable media defeating “air-gap”
- Centrifuges commanded to over speed and operators were sent normal operating plant information
- Destroyed centrifuges and wasted uranium hexafluoride gas affecting Iran’s enrichment capabilities

Kudankulam Nuclear Power Plant

- IT network breached
- Malware introduced through infected employees personnel computer connected to the corporate network
- OT networks are isolated from IT network and not affected
- Large amounts of data exfiltrated
- Attribution likely North Korea



Attack Motives and Examples

- **Monetary Gain**
  - Theft
    - Ransomware, IRS hack, financial institutions
  - Spam and Scams
  - Industrial Espionage / Business Competition
- **Cyberwarfare**
  - Trisis, Stuxnet, Havex, BlackEnergy, Industroyer
  - Espionage
    - Solarwinds (DHS, DOE, DOD, DOJ, Department of State, Department of Commerce, Treasury, NIH, and at least up to 200 total federal and private organizations)
    - China breach of Equifax and OPM
  - Anti-terrorism (takedown of Al Qaeda infrastructure)
  - FBI take downs of criminal networks
- **Other**
  - "Hacktivism"
  - The challenge and notoriety
  - White Hat

Image source: fbi.gov/news/stories/alphabay-takedown

Attack Sequence

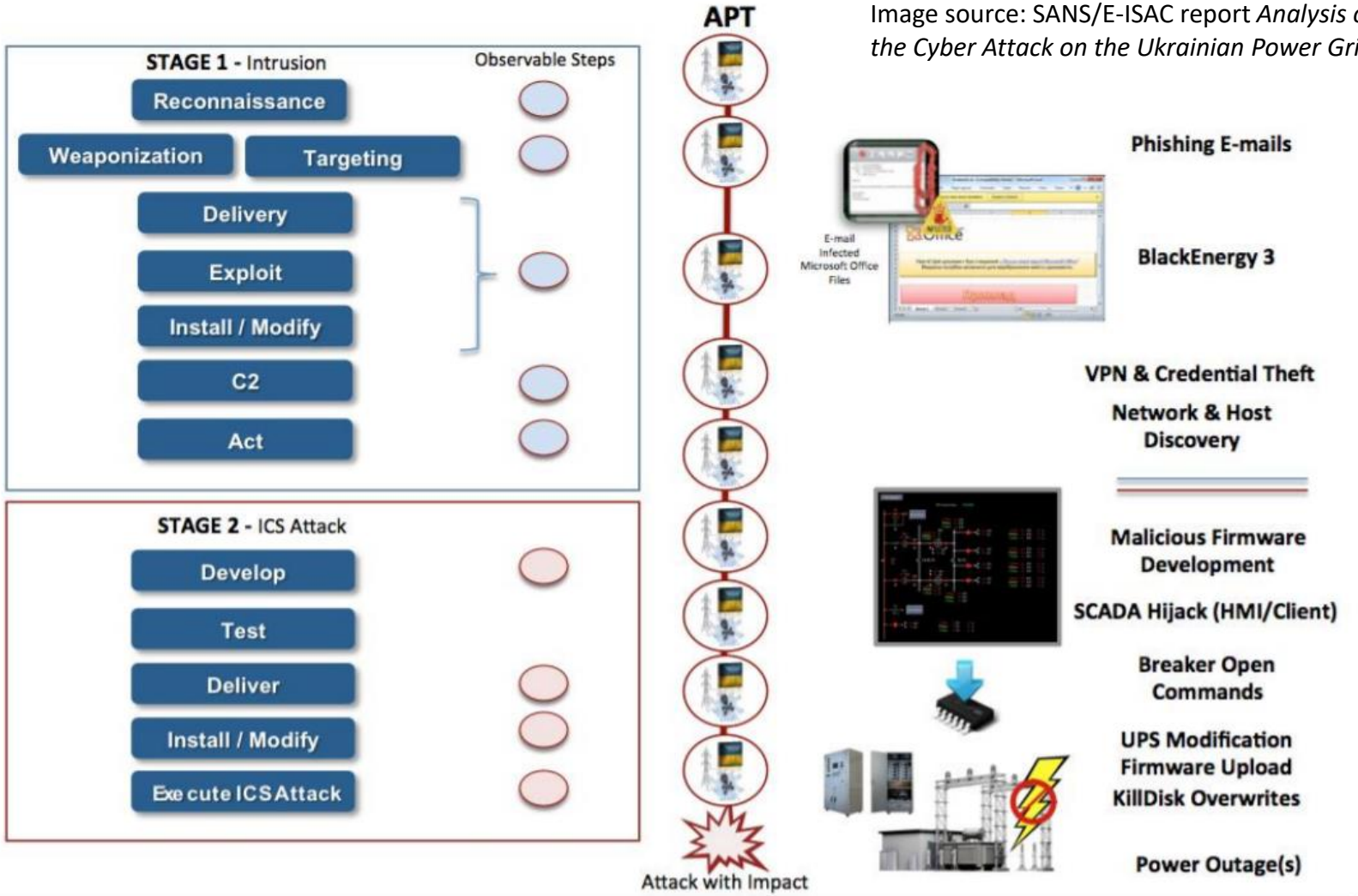


Image source: SANS/E-ISAC report *Analysis of the Cyber Attack on the Ukrainian Power Grid*

Question #1

Who would you consider a threat to the Bulk Electric System?

A. Nation state hacking groups
B. Individual hackers
C. Private hacking groups
D. All of the above
E. A and C

Question #2

What was the most destructive OT attack in history?

A. Stuxnet
B. Ukraine power outage
C. Kudankulam Nuclear Power Plant
D. Saudi Aramco
E. Other

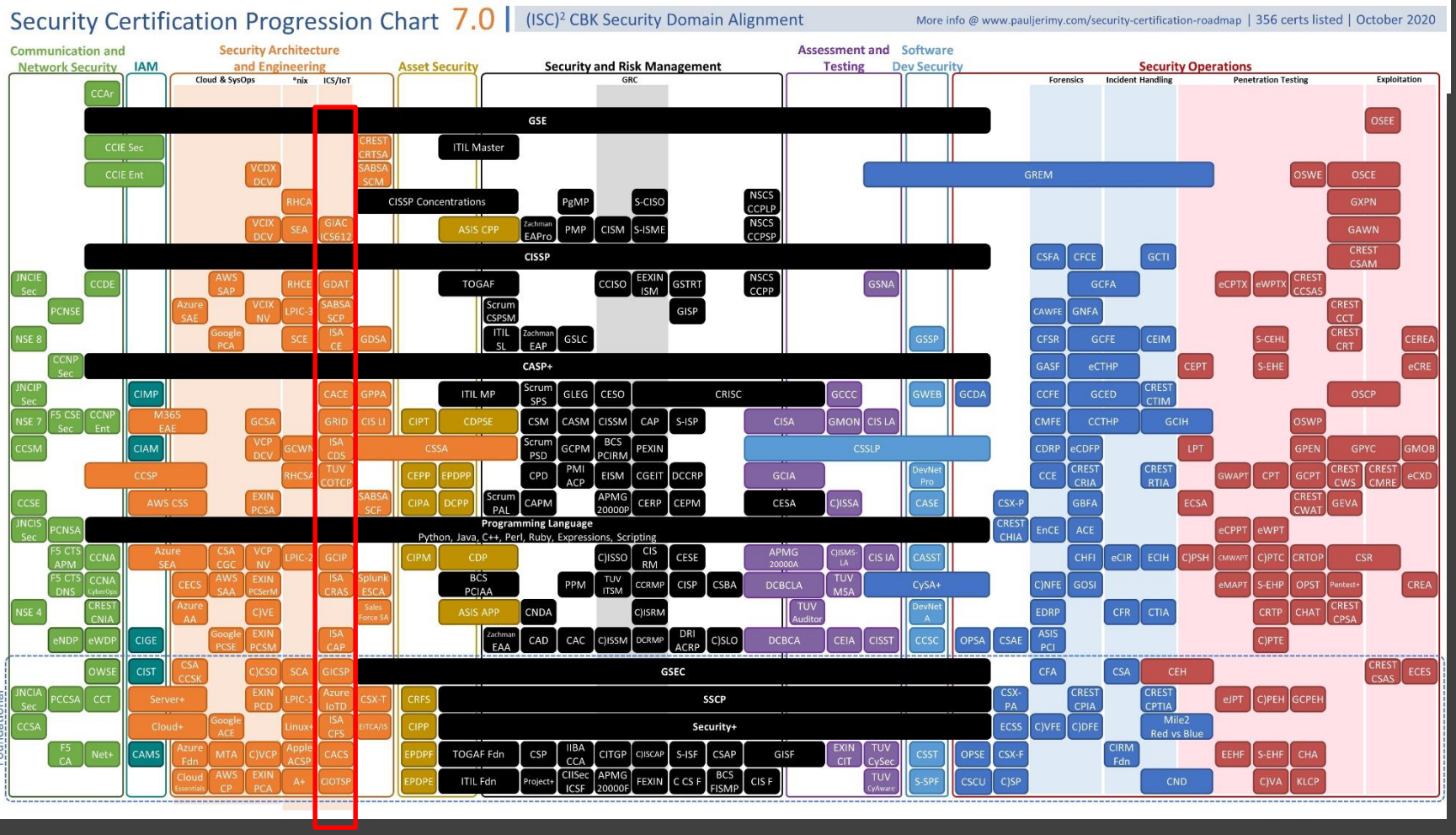
Protecting Against Attacks

- **Cyber Security Triad**
  - Confidential, Integrity, and Availability (CIA)
  - Limit access to information to those authorized
  - Ensure data is accurate and trustworthy
  - Prevent data disruptions
- **NIST Cyber Security Framework**
  - Identify -> Protect -> Detect -> Respond -> Recover
  - Adaptable to many sectors, technologies, and uses
  - Risk Based
  - Covers the full life cycle of cyber security
- **Common Elements**
  - Multi-factor authentication and password managers
  - Security awareness training
  - Security tools – antivirus, firewalls, honeypots, security information and event management (SEIM), vulnerability scanners
  - Patching
  - Data backups
  - Network design

Image source: nist.gov/cyberframework

Available Certifications

Cybersecurity is a large diverse field



Applying Cybersecurity to ICS

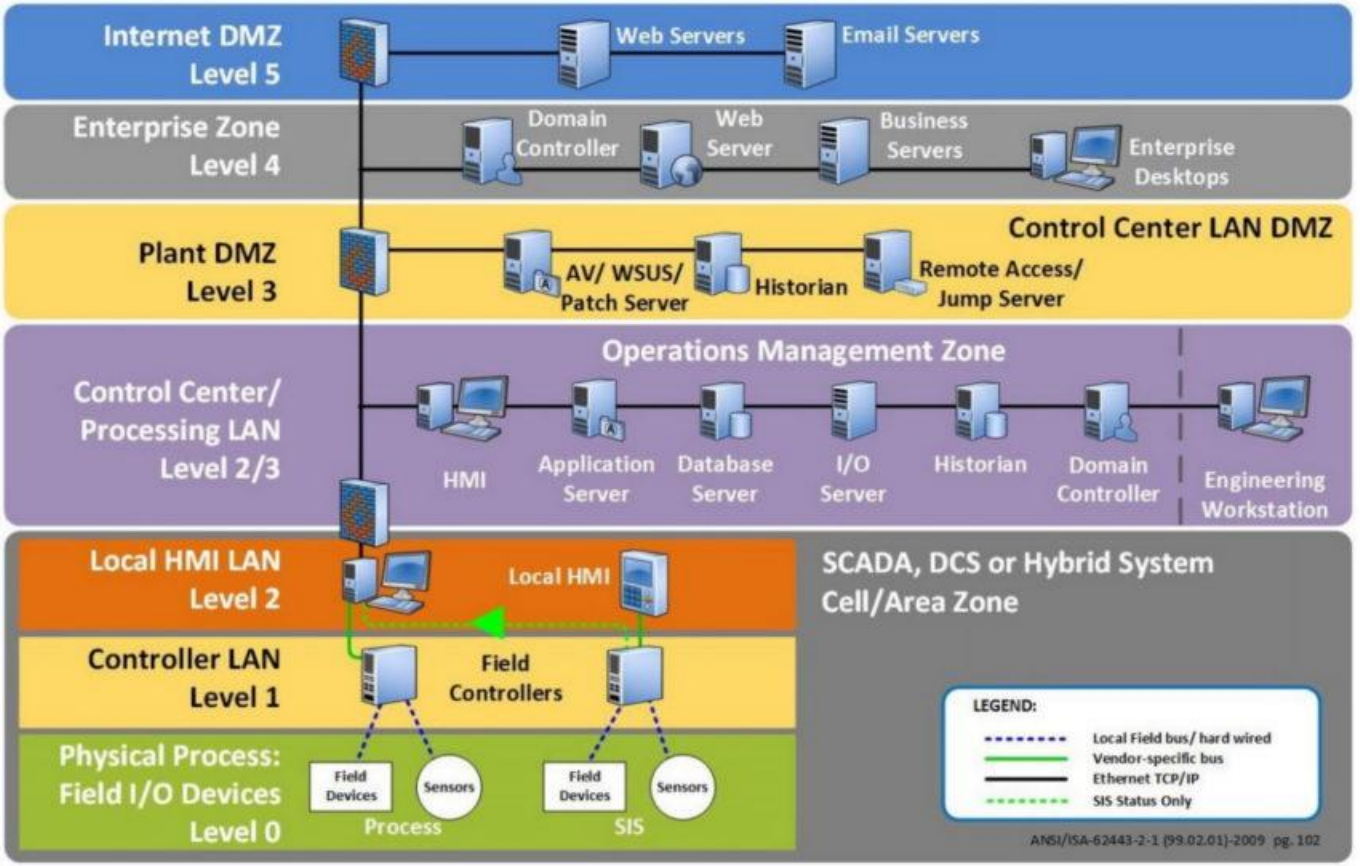
Image source: eaton.com

IT security ≠ OT security

- Equipment lifecycles
- Legacy equipment
- Patching complications
- Different security priorities
- Not supported by traditional cybersecurity tools
- Protocols often lack basic encryption
- OT devices are notoriously insecure
  - Default credentials
  - Insecure factory configurations
  - Remote connectivity often without 2Fa
  - Less than secure coding practices

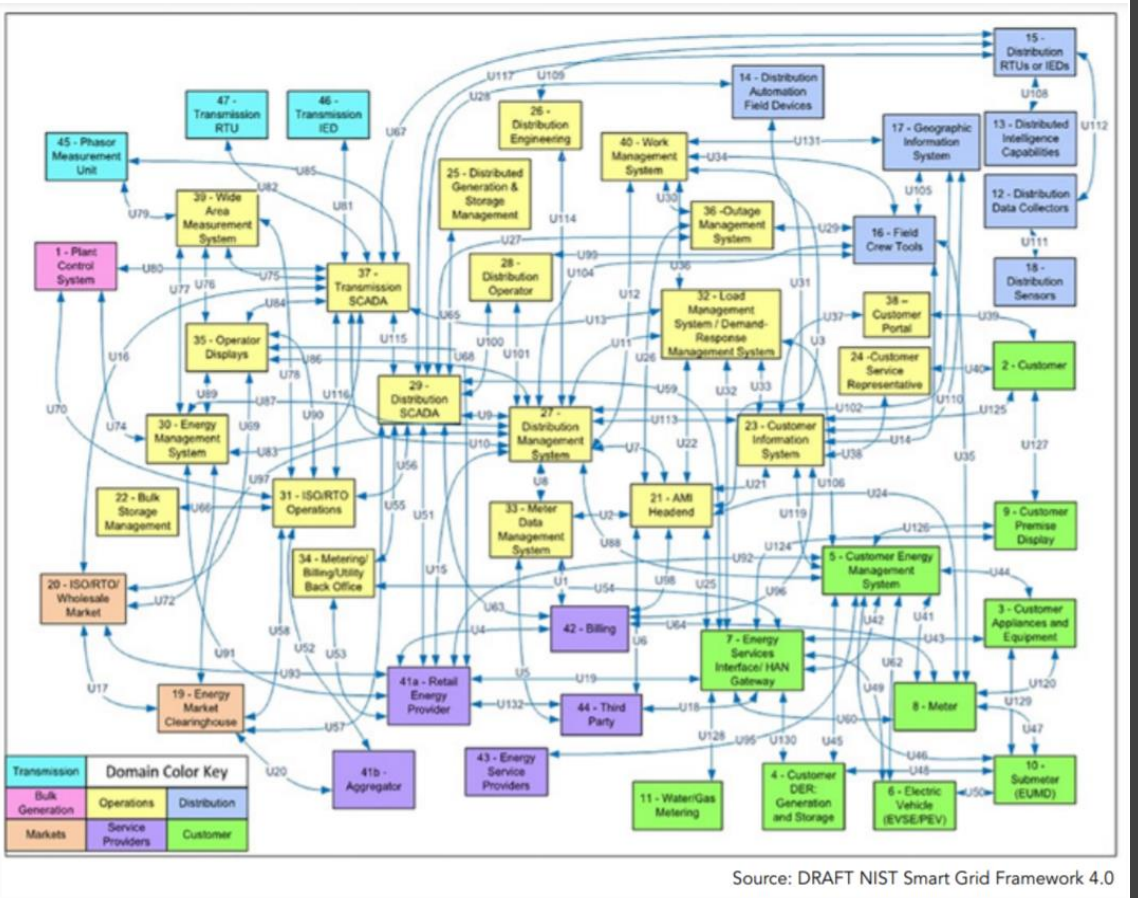
Applying Cybersecurity to Industrial Control Systems (ICS)

- Prioritize Availability and Integrity
- Purdue Model approach – wrap vulnerable equipment in a security blanket



Smart Grid Challenges

- Complex data paths between networks of multiple stakeholders
- Geographically separate facilities requiring routing over public internet (virtual power plant)
- Less forgiving of software errors
  - Loss of grid inertia from large rotating generators
- Highly connected
- Supply chain risk
- Remote control of distributed and diverse assets without standardized approach



Source: DRAFT NIST Smart Grid Framework 4.0

Adapting Security Approach for Smart Grid

- Purdue Model is less effective
- Requires hybrid approach between IT and OT
  - Smart grid equipment conducive to this approach
- Follow published generic organizational and control systems best practices
  - NIST CSF and NIST SP 800-82
  - ISO/IEC 27000 series
  - IEC 62443
- Implement best practices specific to DER
  - NISTIR 7628
  - IEC 62351 series
  - 1547.3 (under development)
- Various research and detailed guidance published by national labs and industry groups

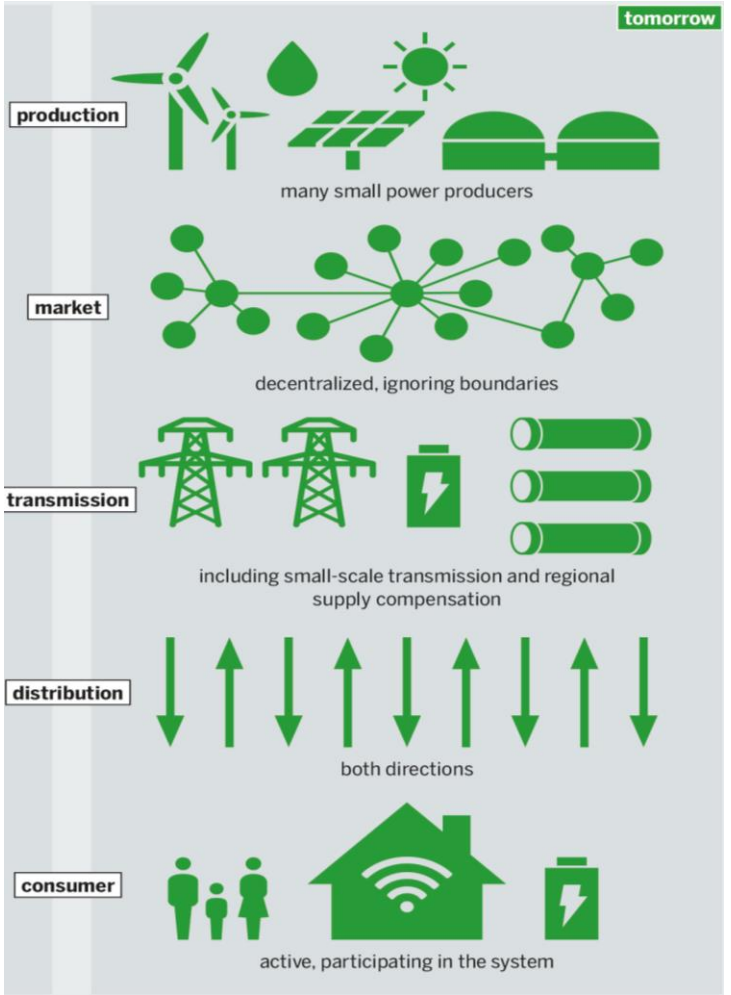


Image source: Wikipedia

But is anyone even targeting the grid?

- Regular phishing attempts
- Black Energy and Havex found in equipment connected to the BES
- Solarwinds
- Industrial espionage at Kudankulam
- Ukraine power grid attacks
- Physical attacks on grid

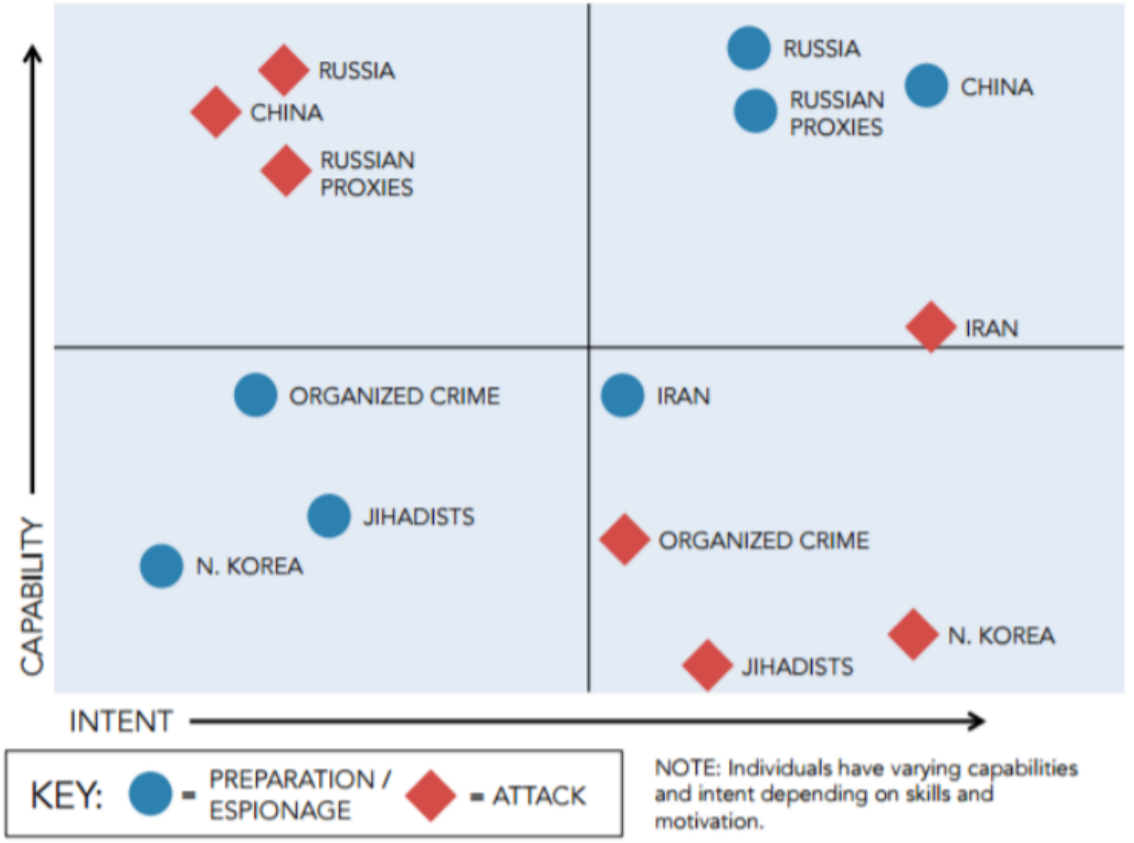


Image source: INL report on Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector for Mission Support Center of DOE

Hard Target

- North American BES is a relatively hard target – for now
  - Good security is a process done iteratively and constantly
- Most of the grid is traditional and relatively secure large generation
- Manual operation backup for switching operations
- Cyber conscious vendors and utilities
- White hat penetration testing of devices and responsible reporting
- NERC CIP
- E-ISAC

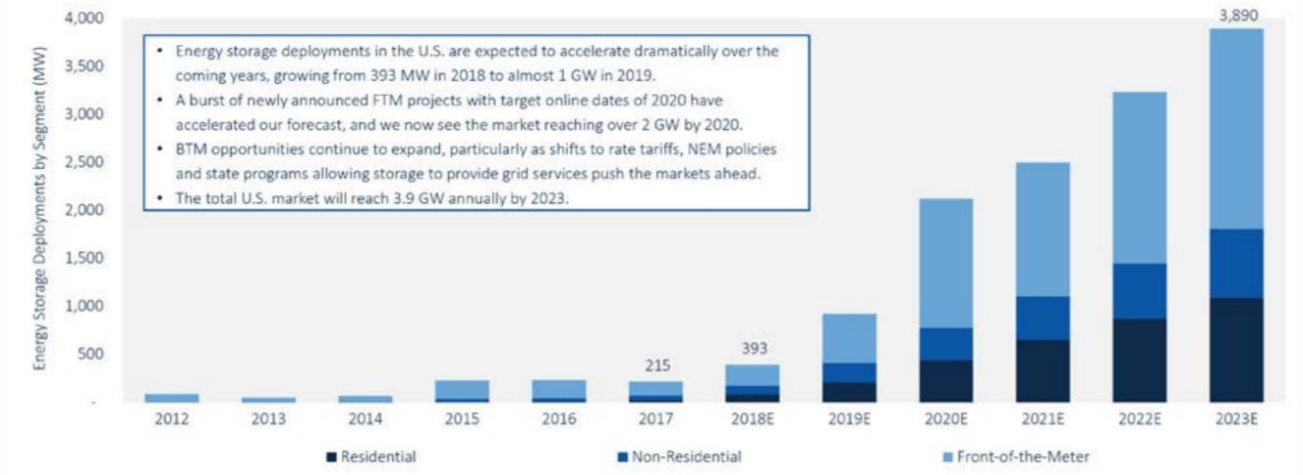


Figure 15. U.S. annual energy storage deployment history (2012–2017) and forecast (2018–2023), in MW, from GTM Research (2018)

Image source: NREL report An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions

Staying Ahead of Threats

- Need to fill the gap between cybersecurity and engineering
  - Improve collaboration between teams
  - OT security teams should include engineers who know security and security staff who know the operation of the system
- Promote security culture across each organization
- Standardized set of comprehensive and industry specific best practices
  - IEEE 1547.3 – only a guideline for first release and not enforceable
- Third party audit and certification for cyber secure devices and systems
  - UL CAP and ISA – but need greater adoption
- Continued research and industry coordination
  - California Rule 21 – need standardized requirements nationwide
  - SunSpec Alliance, IEEE, and other industry groups
  - CISA, NIST, DOE (CESAR and SETO), National Labs, FFRDCs, EPRI

Call to Action

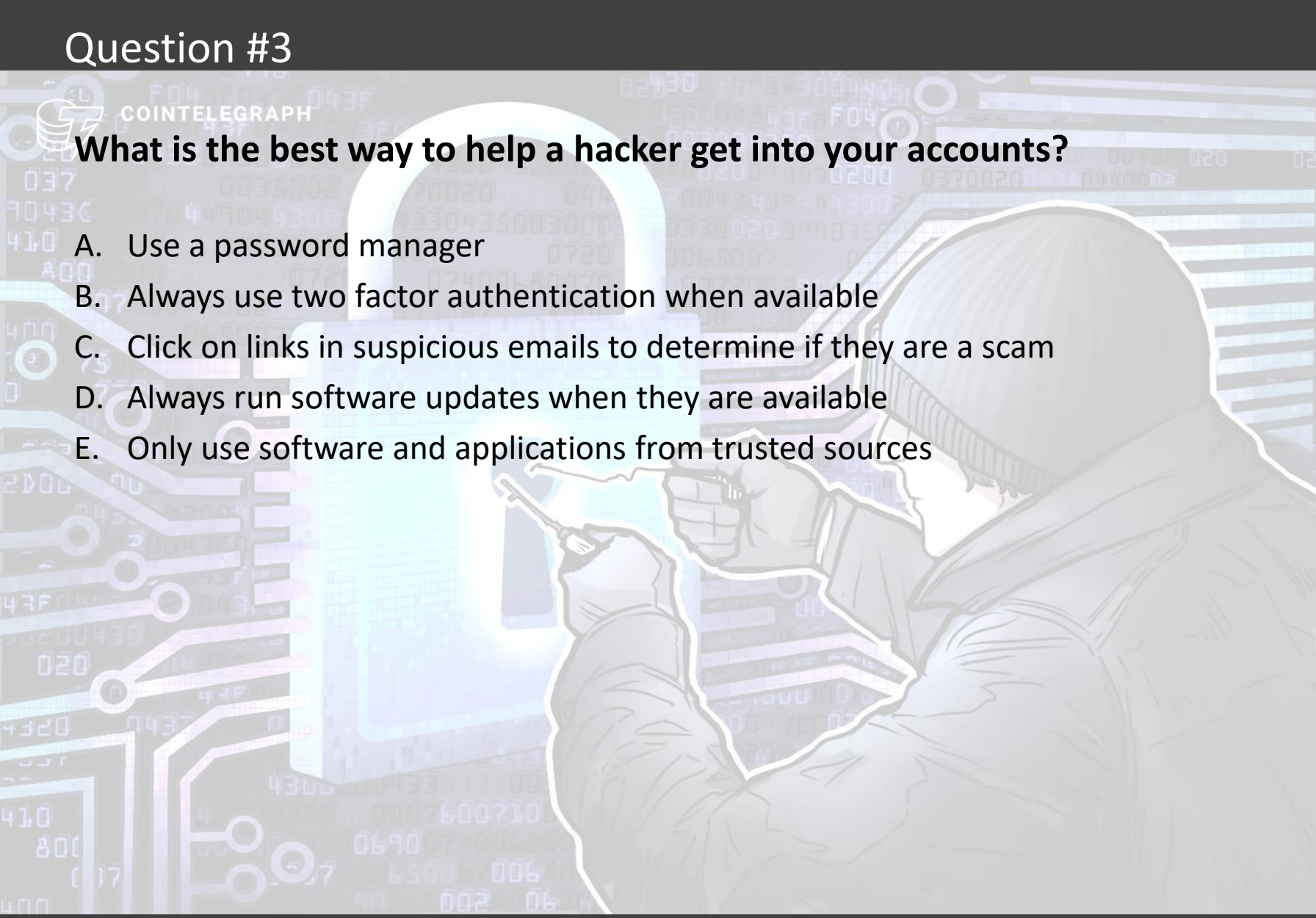
- Develop cyber aware staff with a security culture
- Know your environment and baseline assets and communications
- Know your current security posture and your security goals
- Identify and implement improvements to reach security goals
- Have a response and recovery plan
- Rinse and repeat

Question #3

COINTELEGRAPH

What is the best way to help a hacker get into your accounts?

A. Use a password manager
B. Always use two factor authentication when available
C. Click on links in suspicious emails to determine if they are a scam
D. Always run software updates when they are available
E. Only use software and applications from trusted sources



BACK UP SLIDES

Supply Chain Risks

- Why are multiple stakeholders an issue?
  - Increases attack surface
  - Little to no control of new attack vectors
  - Complex contractual agreements
  - Require clear and concise division of responsibilities

Executive Order on Securing the Information and Communications Technology and Services Supply Chain
EO 13863 https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

TARGET

FORTINET®

CVE-2018-13379 Detail

solarwinds

Grid Attack Surface is Increasing

- Large number of devices directly connected to the internet
- More communications over the internet
- More diverse set of stakeholders with access

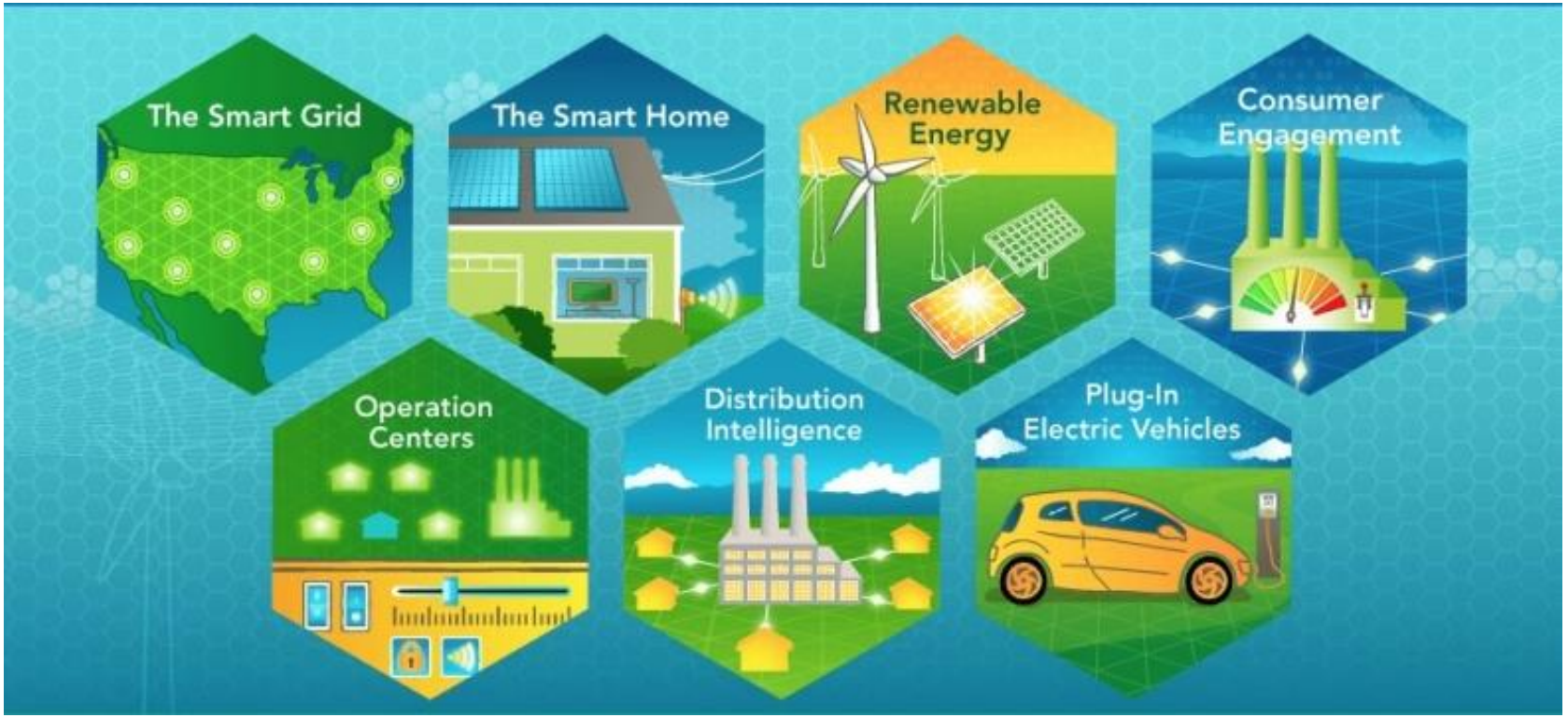


Image source: energy.gov/science-innovation/electric-power/smart-grid