Cyber Threat Landscape for Distribution Systems

Megan Culler, Idaho National Laboratory

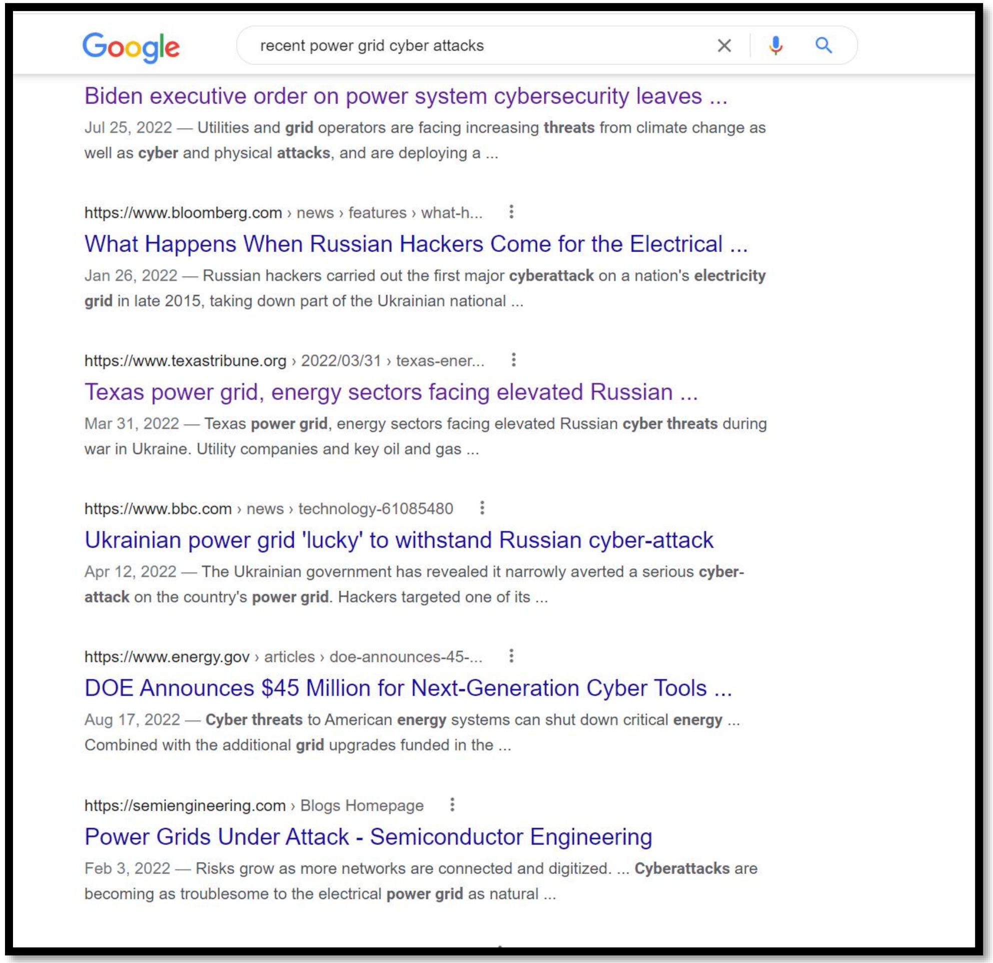
Distribution Conference

October 4-5, 2022

Agenda

- Recent Attacks
- Attack Paths
- Cyber Resilience

Recent Events



recent power grid cyber attacks

Biden executive order on power system cybersecurity leaves ...

Jul 25, 2022 — Utilities and **grid** operators are facing increasing **threats** from climate change as well as **cyber** and physical **attacks**, and are deploying a ...

https://www.bloomberg.com › news › features › what-h...

What Happens When Russian Hackers Come for the Electrical ...

Jan 26, 2022 — Russian hackers carried out the first major **cyberattack** on a nation's **electricity grid** in late 2015, taking down part of the Ukrainian national ...

https://www.texastribune.org › 2022/03/31 › texas-ener...

Texas power grid, energy sectors facing elevated Russian ...

Mar 31, 2022 — Texas **power grid**, energy sectors facing elevated Russian **cyber threats** during war in Ukraine. Utility companies and key oil and gas ...

https://www.bbc.com › news › technology-61085480

Ukrainian power grid 'lucky' to withstand Russian cyber-attack

Apr 12, 2022 — The Ukrainian government has revealed it narrowly averted a serious **cyber-attack** on the country's **power grid**. Hackers targeted one of its ...

https://www.energy.gov › articles › doe-announces-45-...

DOE Announces $45 Million for Next-Generation Cyber Tools ...

Aug 17, 2022 — **Cyber threats** to American **energy** systems can shut down critical **energy** ... Combined with the additional **grid** upgrades funded in the ...

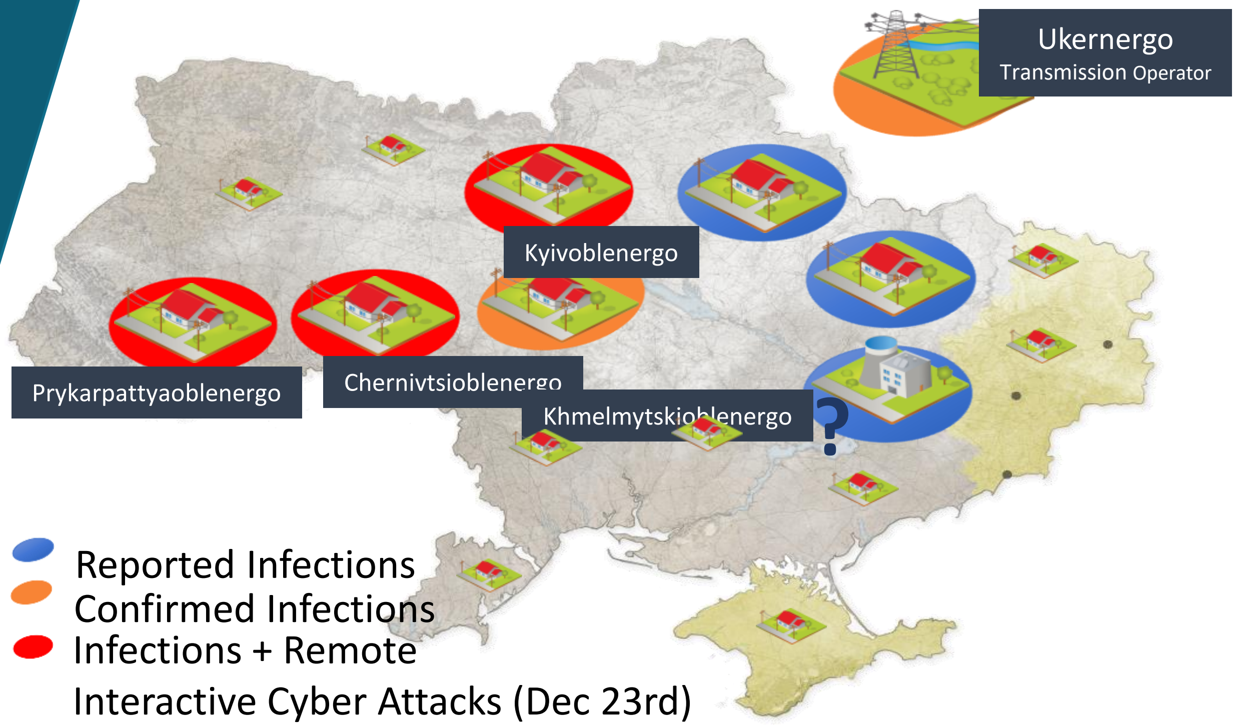
https://semiengineering.com › Blogs Homepage

Power Grids Under Attack - Semiconductor Engineering

Feb 3, 2022 — Risks grow as more networks are connected and digitized. ... **Cyberattacks** are becoming as troublesome to the electrical **power grid** as natural ...

Recent Events

Attacks on Ukrainian Power Grid



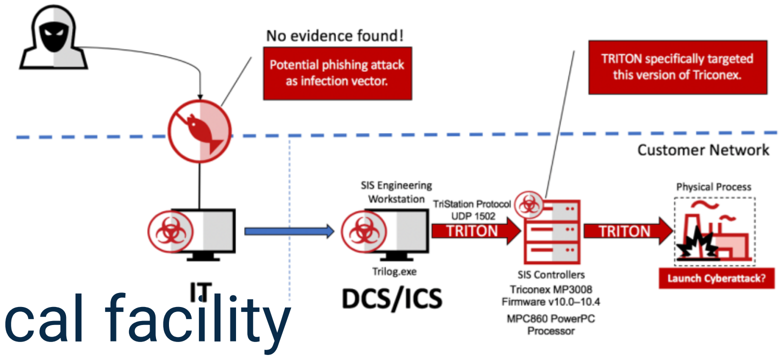
- 🟦 Reported Infections
- 🟧 Confirmed Infections
- 🟥 Infections + Remote Interactive Cyber Attacks (Dec 23rd)

- 2015 Attack on distribution:
  - BlackEnergy
- 2016 Attack on transmission:
  - Industroyer/Crash Override

Image: INL

Recent Events

Malware that targets OT systems



- Triton
  - First seen in 2017 at a petrochemical facility
  - Designed to manipulate safety instrumented systems (SIS)
  - Same threat actor discovered probing networks of electricity organizations in US and elsewhere in 2018
  - FBI released report in March 2022 warning of ongoing Triton Threat
- Incontroller/ PipeDream
  - Discovered in early 2022
  - Collection of utilities that includes reconnaissance, manipulation, disruption of PLCs

Recent Events

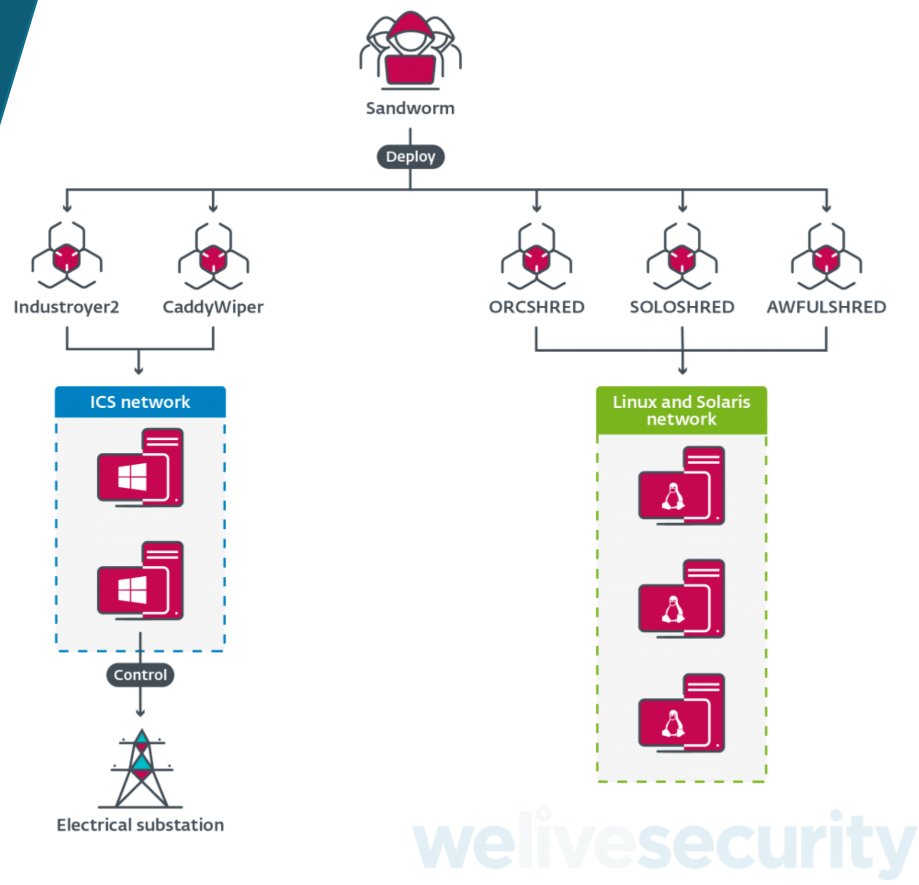
sPower - 2019

- Utah-based renewable IPP sPower
- Firewalls hit with DoS attack
- Affected Cisco firewall in 5-minute intervals over 12-hour period
- Equipment targeted was on the public internet
- Attacker was likely not targeted electric infrastructure

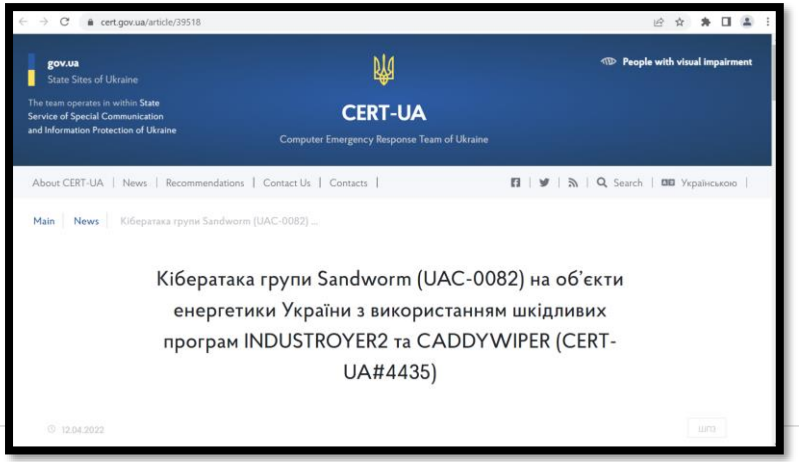
Image: Cisco

Recent Events

Industryoyer2



- Single ICS protocol targeted: IEC-104 (IEC 60870-40104)
- Attack detected and mitigated before blackout occurred
- Could have impacted ~2 million people
- Several wipers deployed


cert.gov.ua/article/39518
People with visual impairment
About CERT-UA | News | Recommendations | Contact Us | Contacts |
Search | Українською |
Main | News | Кібератака групи Sandworm (UAC-0082) ...
12.04.2022

gov.ua
State Sites of Ukraine

The team operates in within State Service of Special Communication and Information Protection of Ukraine

CERT-UA

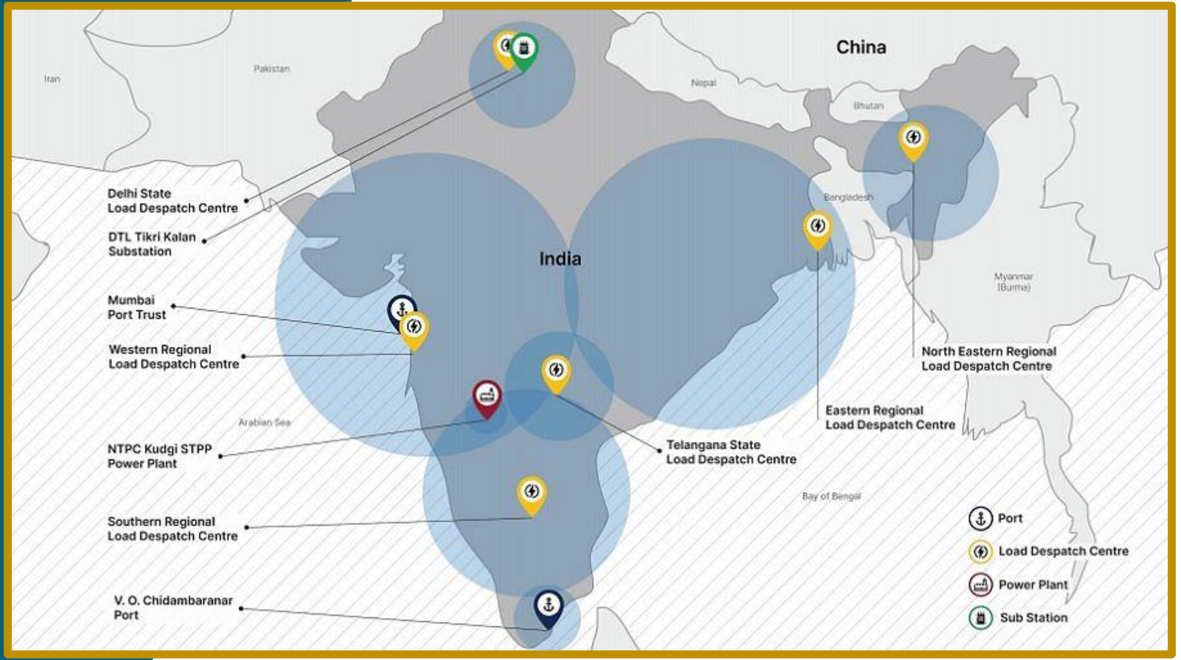
Computer Emergency Response Team of Ukraine

Кібератака групи Sandworm (UAC-0082) на об'єкти енергетики України з використанням шкідливих програм INDUSTROYER2 та CADDYWIPER (CERT-UA#4435)

Image: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
https://cert.gov.ua/article/39518

Recent Events

Attacks on Indian Transmission


Iran
Pakistan
Nepal
China
Bhutan
Bangladesh
India
Myanmar (Burma)
Arabian Sea
Bay of Bengal
Delhi State Load Despatch Centre
DTL Tikri Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
NTPC Kudgi STPP Power Plant
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port
Telangana State Load Despatch Centre
Eastern Regional Load Despatch Centre
North Eastern Regional Load Despatch Centre
Port
Load Despatch Centre
Power Plant
Sub Station

- Feb. 2021: reported that since mid-2020, Chinese APTgroup RedEcho compromised at least 10 Indian power sector organizations
- Targets included 4 of 5 Regional Load Dispatch Centers (RLDC)
- No compromise of OT network, but info could be leveraged for larger campaign

Image: Recorded Future
https://www.recordedfuture.com/redecho-targeting-indian-power-sector

Recent Events

Attacks on Indian Transmission

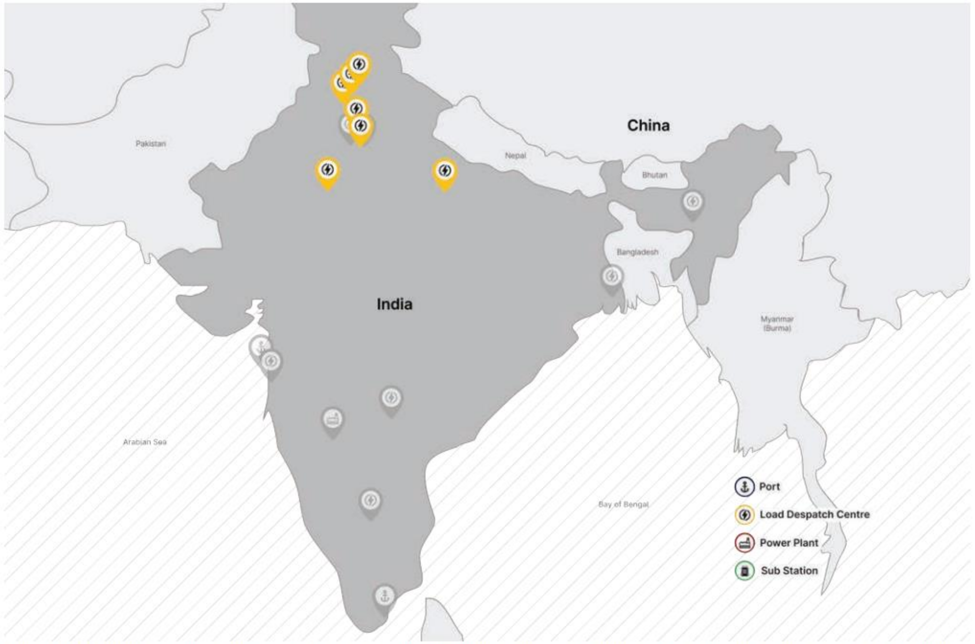


Figure 4: Map of TAG-38 victim State Load Despatch Centre (SLDC) locations. Previously reported RedEcho victim locations also displayed in gray (Source: Recorded Future)

Threat Activity Group (TAG)-38

- April 2022, reported that since Sept. 2021, Chinese campaign targeted at least 7 State Load Dispatch Centers (SLDCs) in North India
- Similar to RedEcho, but entry point was internet-facing, third-party DVR/IP camera devices as C2 for Shadowpad malware
- No compromise of OT network, but access info on critical infrastructure

Image: Recorded Future
https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets

Recent Events

Wind in Europe

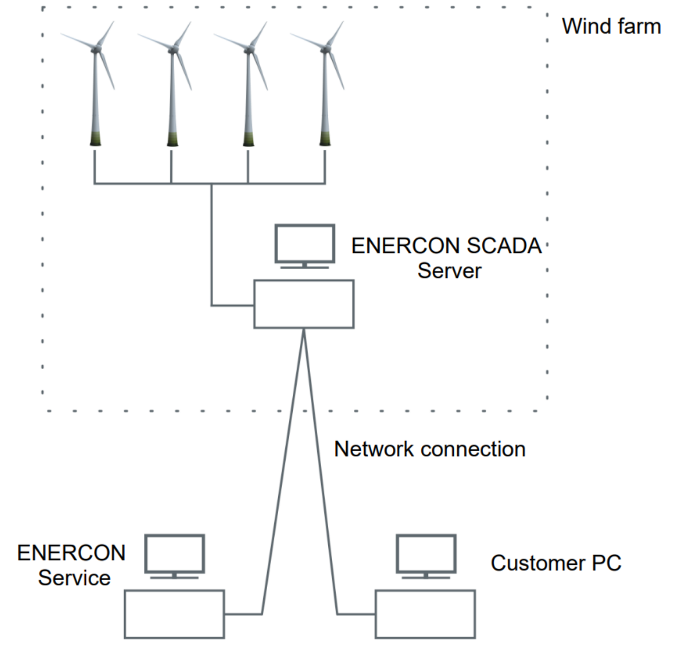


Fig. 1: Schematic structure of ENERCON SCADA system

- Nov. 19, 2021: Vestas hit by ransomware
- Feb. 24, 2022: Enercon wind turbines in Germany lose remote monitoring connection due to SATCOM attack
- March 31, 2022: Nordex Group, major wind turbine manufacturer, hit by Conti ransomware
- April 11, 2022: Deutsche Windtechnik, wind turbine maintenance company, hit by cyber attack

Recent Events

State-sponsored activity against the North American Electricity Sector

- Iranian state-sponsored espionage campaign (2019)
- U.S. utilities targeted by TA410 (2019)
- Russian group behind Triton probing U.S. utilities (2019)
- U.S. DHS and FBI alerts on Russian-state sponsored targeting of supply chain (2018 and ongoing)
- Russian state-sponsored cyber espionage against Canadian, US, and European energy sector companies (2014-2017)
- U.S. power producer with generation plan in Ontario probed by multiple actors (2013)
- Grid software supplier Televant Canada Ltd. had project files related to ICS software stolen (2012)

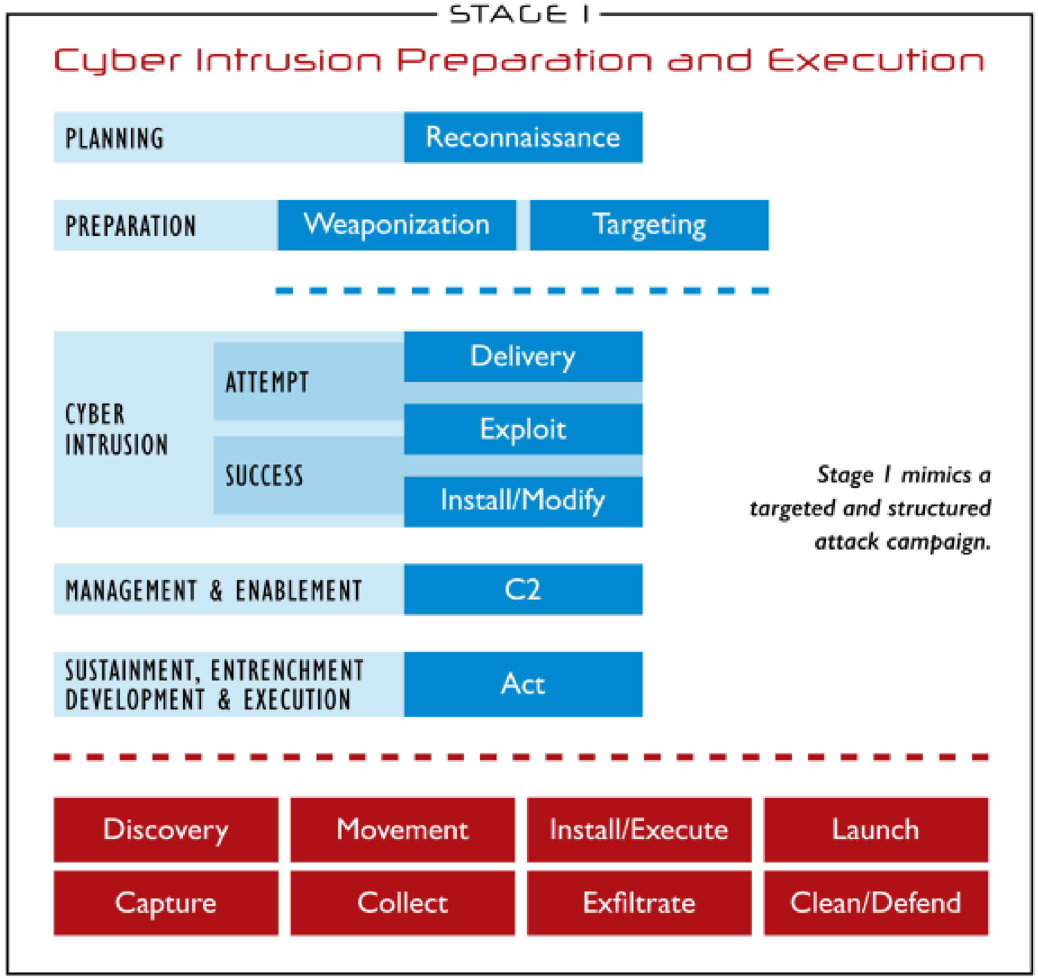
Image: Recorded Future
https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets

Recent Events

Common Themes

- Attacks targeting third parties (OEMs, maintenance, etc.)
- APT activity detected before OT attack executed
- Some attacks are not targeting electric infrastructure
- Few notable incidents that shut down power operations

Attack Paths



STAGE 1

Cyber Intrusion Preparation and Execution

PLANNING: Reconnaissance

PREPARATION: Weaponization, Targeting

CYBER INTRUSION
- ATTEMPT: Delivery
- SUCCESS: Exploit, Install/Modify

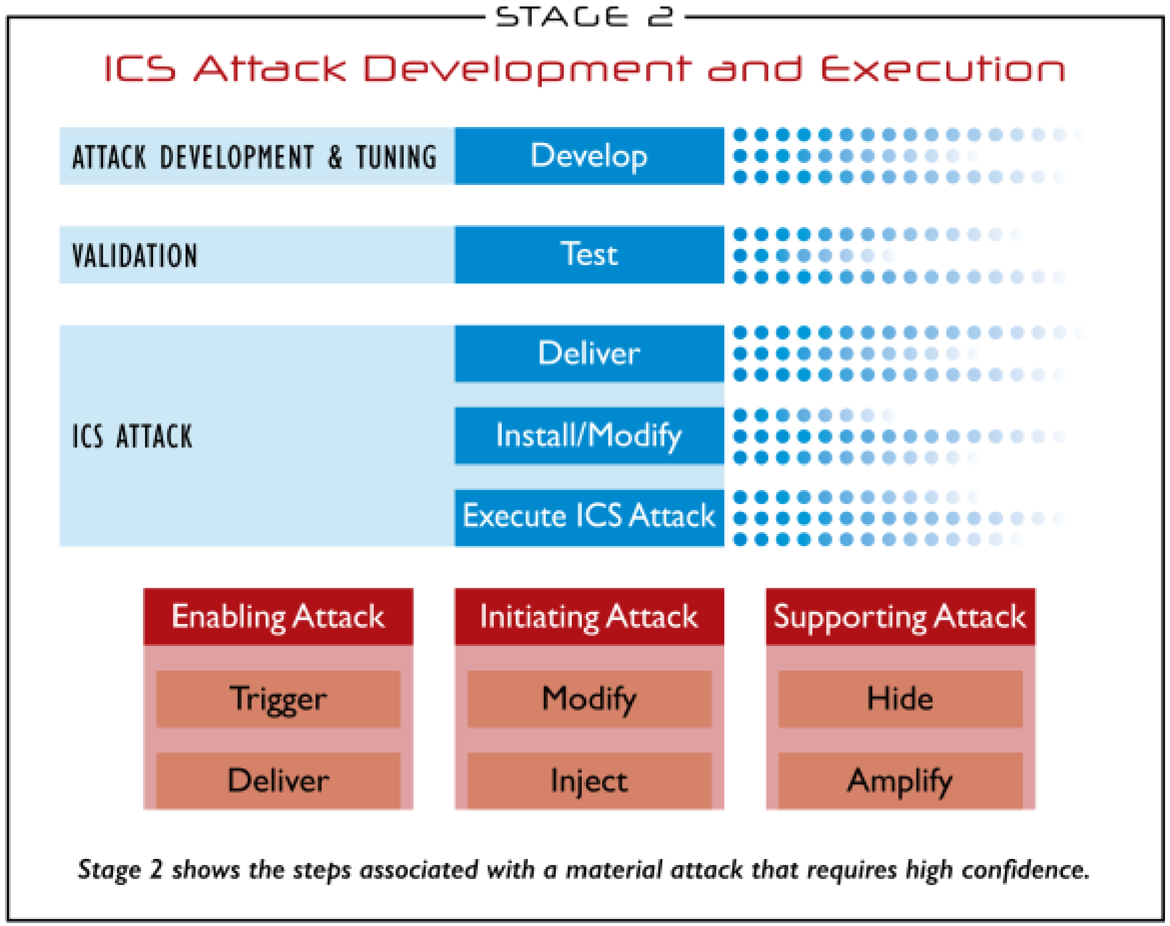
MANAGEMENT & ENABLEMENT: C2

SUSTAINMENT, ENTRENCHMENT DEVELOPMENT & EXECUTION: Act

Discovery, Movement, Install/Execute, Launch

Capture, Collect, Exfiltrate, Clean/Defend

Stage 1 mimics a targeted and structured attack campaign.



STAGE 2

ICS Attack Development and Execution

ATTACK DEVELOPMENT & TUNING: Develop

VALIDATION: Test

ICS ATTACK: Deliver, Install/Modify, Execute ICS Attack

Enabling Attack: Trigger, Deliver

Initiating Attack: Modify, Inject

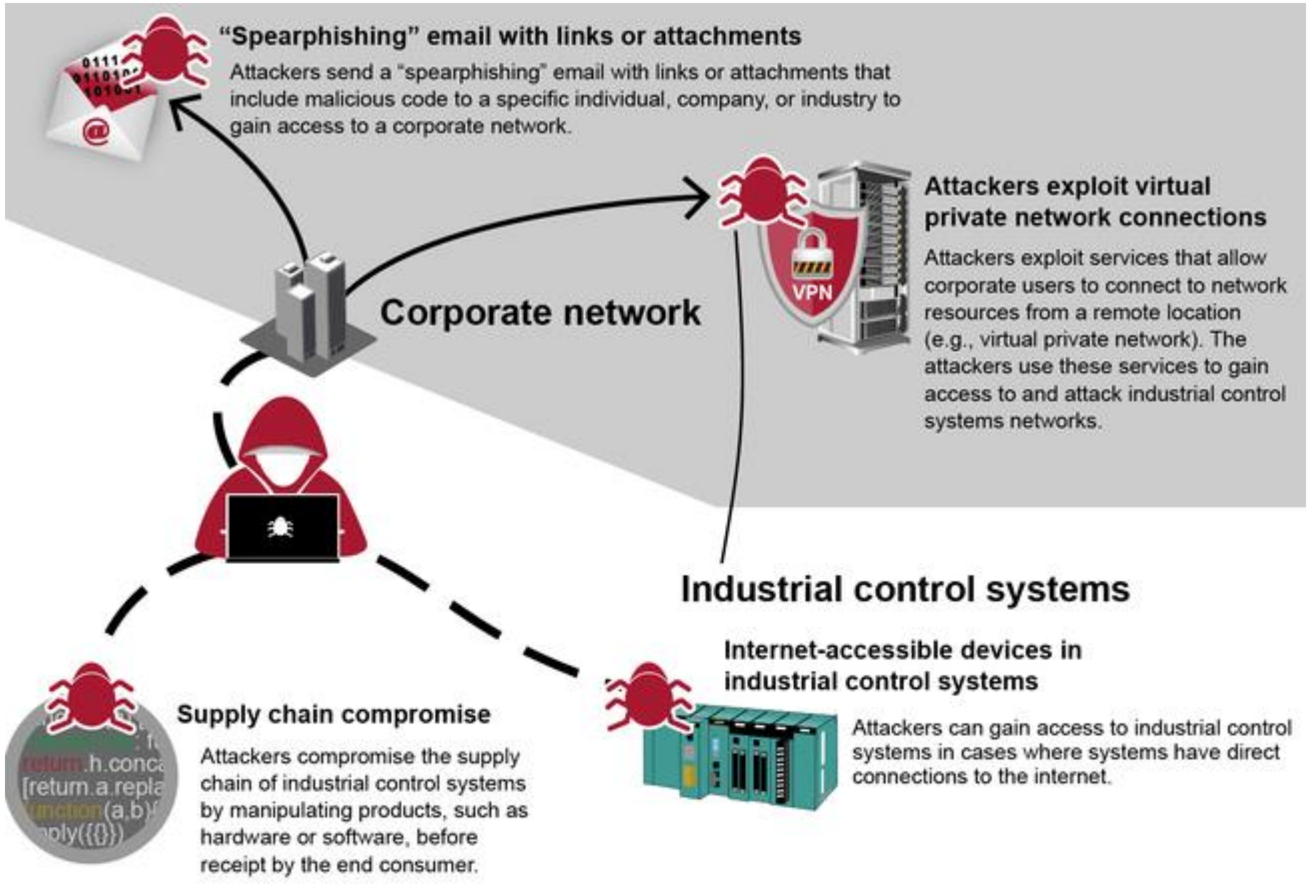
Supporting Attack: Hide, Amplify

Stage 2 shows the steps associated with a material attack that requires high confidence.

Based on the Cyber Kill Chain® model from Lockheed Martin

Attack Types

Entry Points to ICS



"Spearphishing" email with links or attachments

Attackers send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network.

Attackers exploit virtual private network connections

Attackers exploit services that allow corporate users to connect to network resources from a remote location (e.g., virtual private network). The attackers use these services to gain access to and attack industrial control systems networks.

Internet-accessible devices in industrial control systems

Attackers can gain access to industrial control systems in cases where systems have direct connections to the internet.

Supply chain compromise

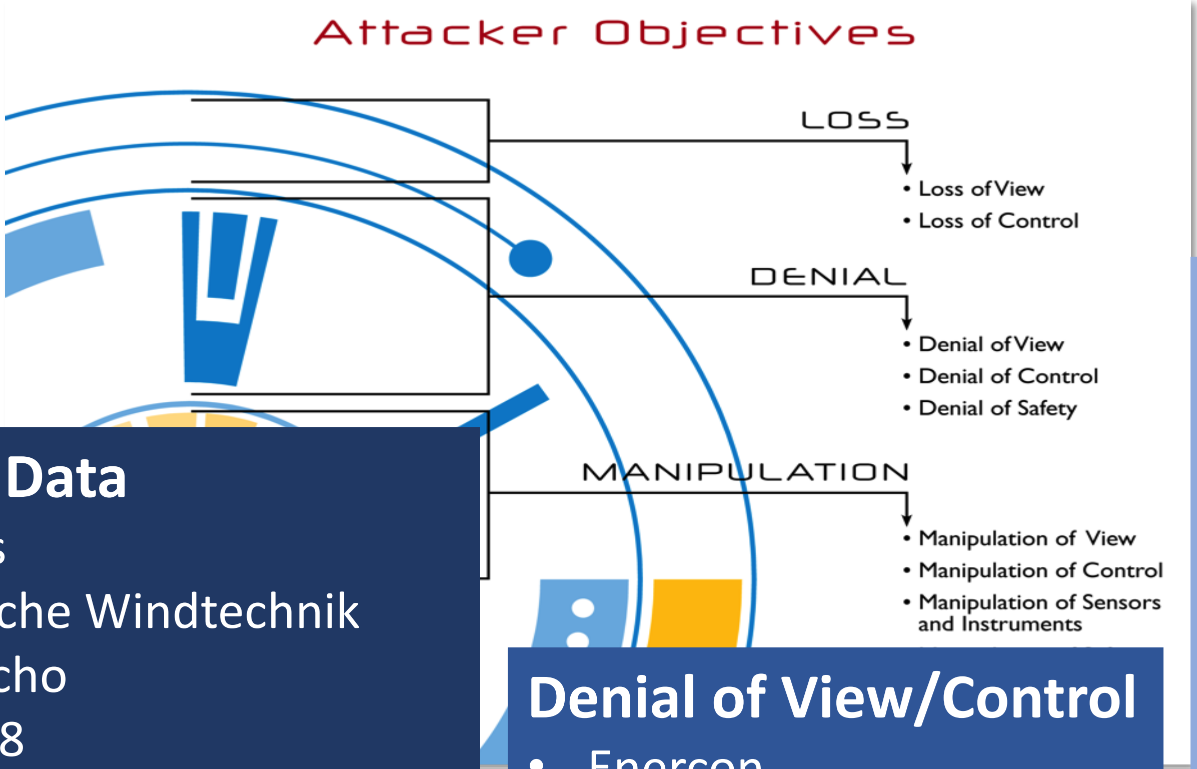
Attackers compromise the supply chain of industrial control systems by manipulating products, such as hardware or software, before receipt by the end consumer.

Source: GAO analysis of industry and federal documents. | GAO-21-81

Image: U.S. Government Accountability Office
https://www.gao.gov/assets/gao-21-81.pdf

Attack Types

Impacts



Attacker Objectives

LOSS

- Loss of View
- Loss of Control

DENIAL

- Denial of View
- Denial of Control
- Denial of Safety

MANIPULATION

- Manipulation of View
- Manipulation of Control
- Manipulation of Sensors and Instruments

Loss of Data

- Vestas
- Deutsche Windtechnik
- Red Echo
- TAG-38

Loss of View/Control

- Nordex
- Deutsche Windtechnik

Denial of View/Control

- Enercon
- Spower

Denial of Safety

- Incontroller
- Triton / Trisis

Manipulation of View

- Stuxnet
- Wipers

Manipulation of Control

- Black Energy
- Industroyer
- Industroyer2

Manipulation of Safety

- Incontroller
- Triton / Trisis

Attack Types

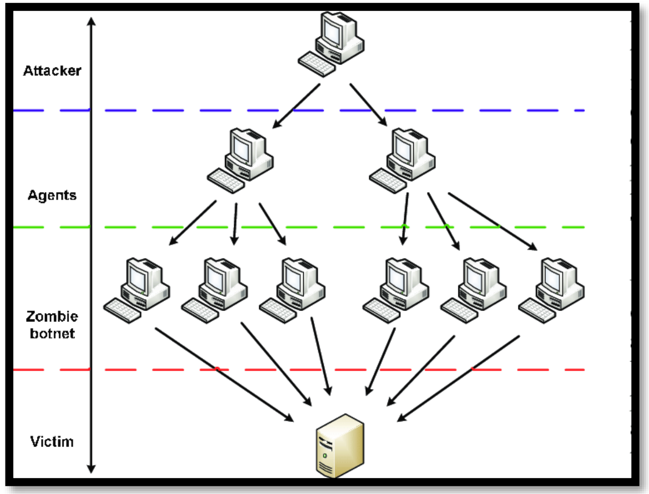
Denial-of-Service

Definition

- Legitimate users are unable to access information systems, devices or other network resources due to actions of malicious actor

Key Considerations

- What backups for critical services are in place?
- How will my system continue to operate autonomously or enter a fail-safe state?



Attack Paths

Ransomware

Definition

- Ransomware is a type of malware that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee

Key Considerations

- Data may be exfiltrated as it's encrypted on local systems
- What data/processes were affected?
- How are these data/processes used across my business?
- What third parties have access to sensitive information?

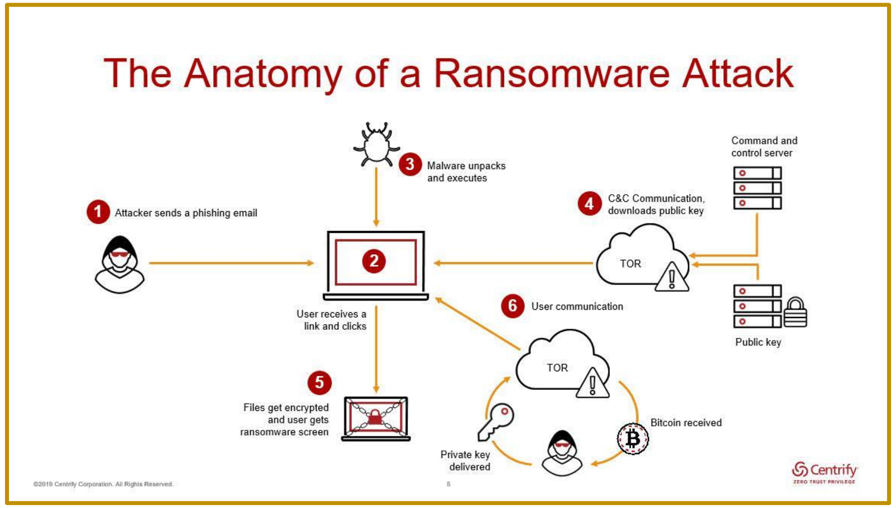

The Anatomy of a Ransomware Attack
1 Attacker sends a phishing email
2
User receives a link and clicks
3 Malware unpacks and executes
4 C&C Communication, downloads public key
Command and control server
TOR
Public key
5 Files get encrypted and user gets ransomware screen
6 User communication
TOR
Bitcoin received
Private key delivered
©2019 Centrify Corporation. All Rights Reserved.
5
Centrify ZERO TRUST PRIVILEGE

Image: Forbes

Attack Paths

Advanced Persistent Threats (APTs)

Definition

- Prolonged and targeted cyberattack that uses continuous and sophisticated hacking techniques to gain access and maintain persistence prior to executing a payload

Key Considerations

- How am I checking for unusual activity?
- How am I ensuring I'm not susceptible to known attacks?

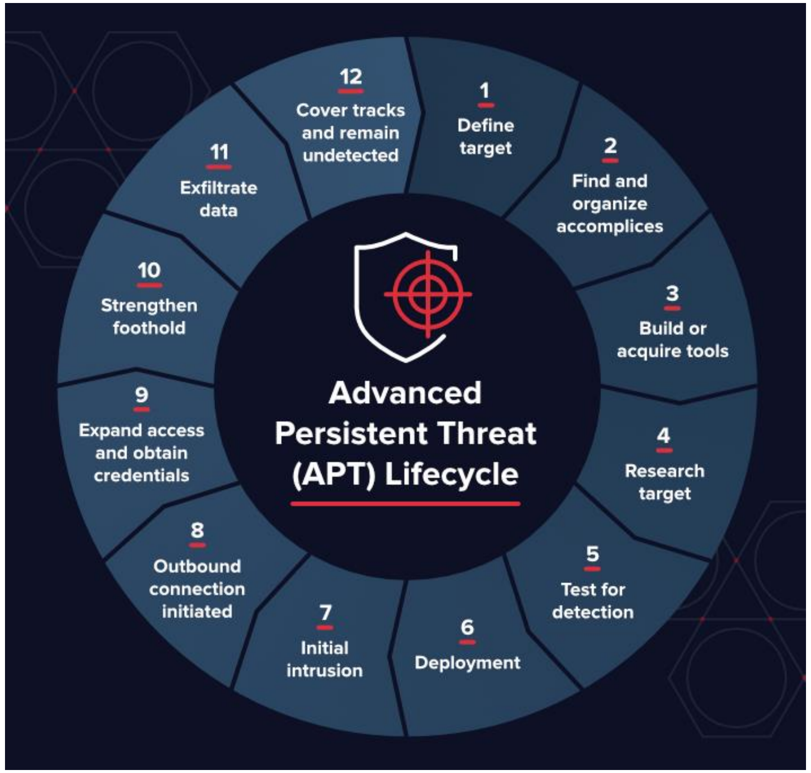
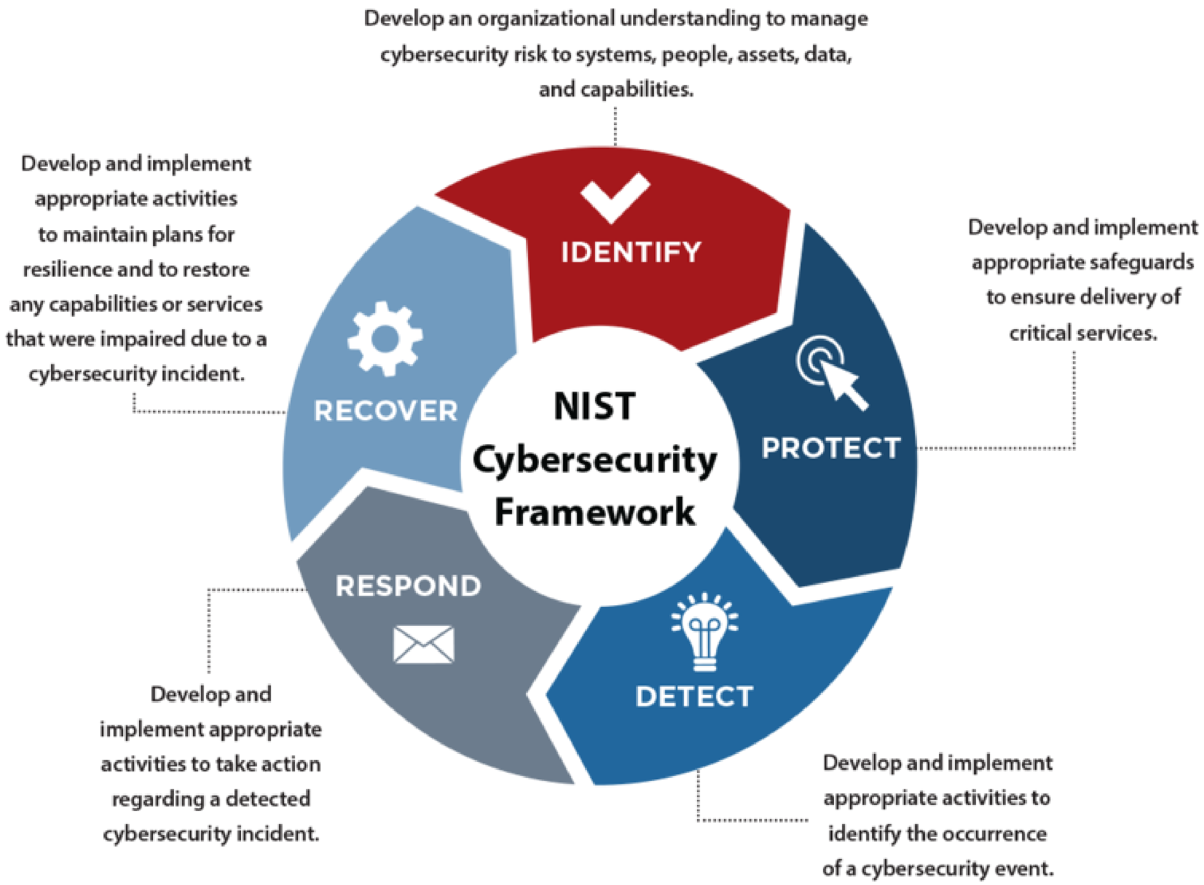

Advanced Persistent Threat (APT) Lifecycle
1 Define target
2 Find and organize accomplices
3 Build or acquire tools
4 Research target
5 Test for detection
6 Deployment
7 Initial intrusion
8 Outbound connection initiated
9 Expand access and obtain credentials
10 Strengthen foothold
11 Exfiltrate data
12 Cover tracks and remain undetected

Image: Varonis

Cyber Resilience



NIST Cybersecurity Framework

IDENTIFY

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

PROTECT

Develop and implement appropriate safeguards to ensure delivery of critical services.

DETECT

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

RESPOND

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

RECOVER

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

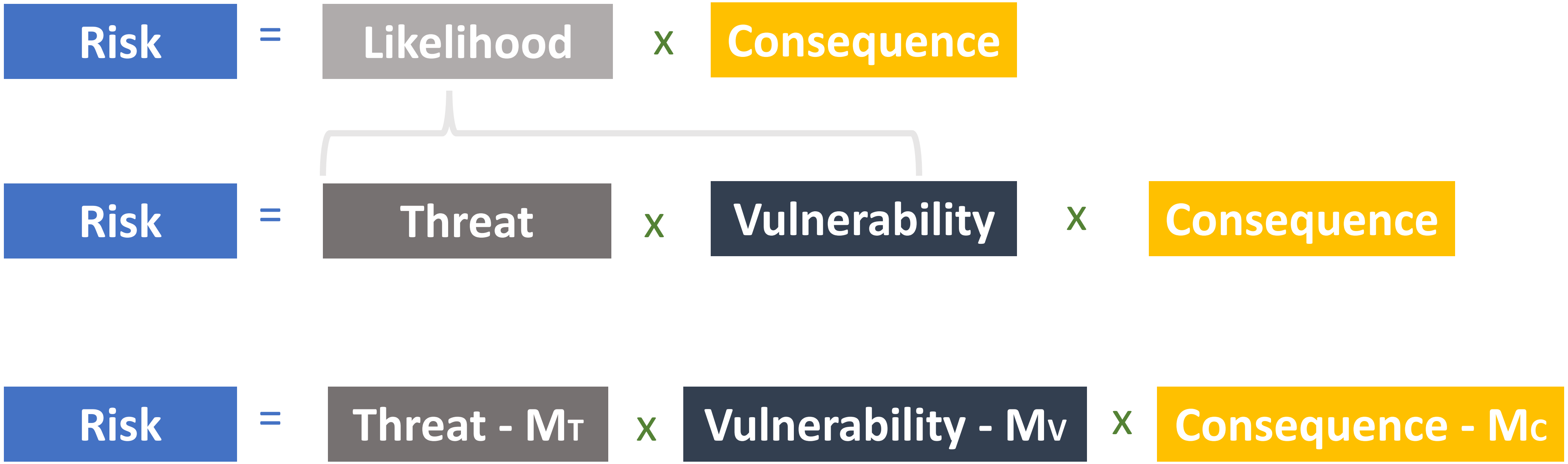
Image: NIST

INL/CON-22-69048

Cyber Resilience

Cyber Risk

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5



Risk = Likelihood x Consequence

Risk = Threat x Vulnerability x Consequence

Risk = Threat - M_T x Vulnerability - M_V x Consequence - M_C

Cyber Resilience

Threats

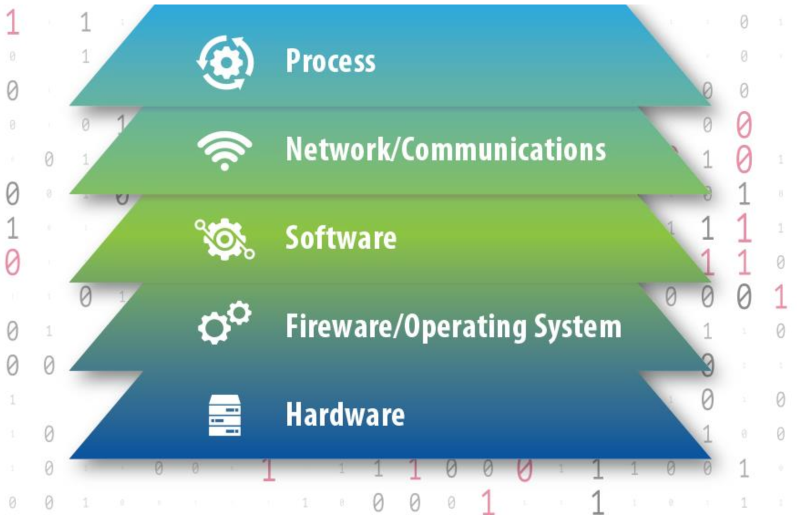
Threat = Intent x Capability x Opportunity

- **Intent:** may be intentional (driven by a particular objective) or unintentional
- **Capability:** skills and funding
- **Opportunity:** Access to a target

Capability	Example
Hacker	Spower Firewall DoS attacker
Insider	AWEA technician
Organized group	Russian cybercrime/ransomware
Hostile nation-state or terrorist	Chinese-sponsored recon of Indian power grid

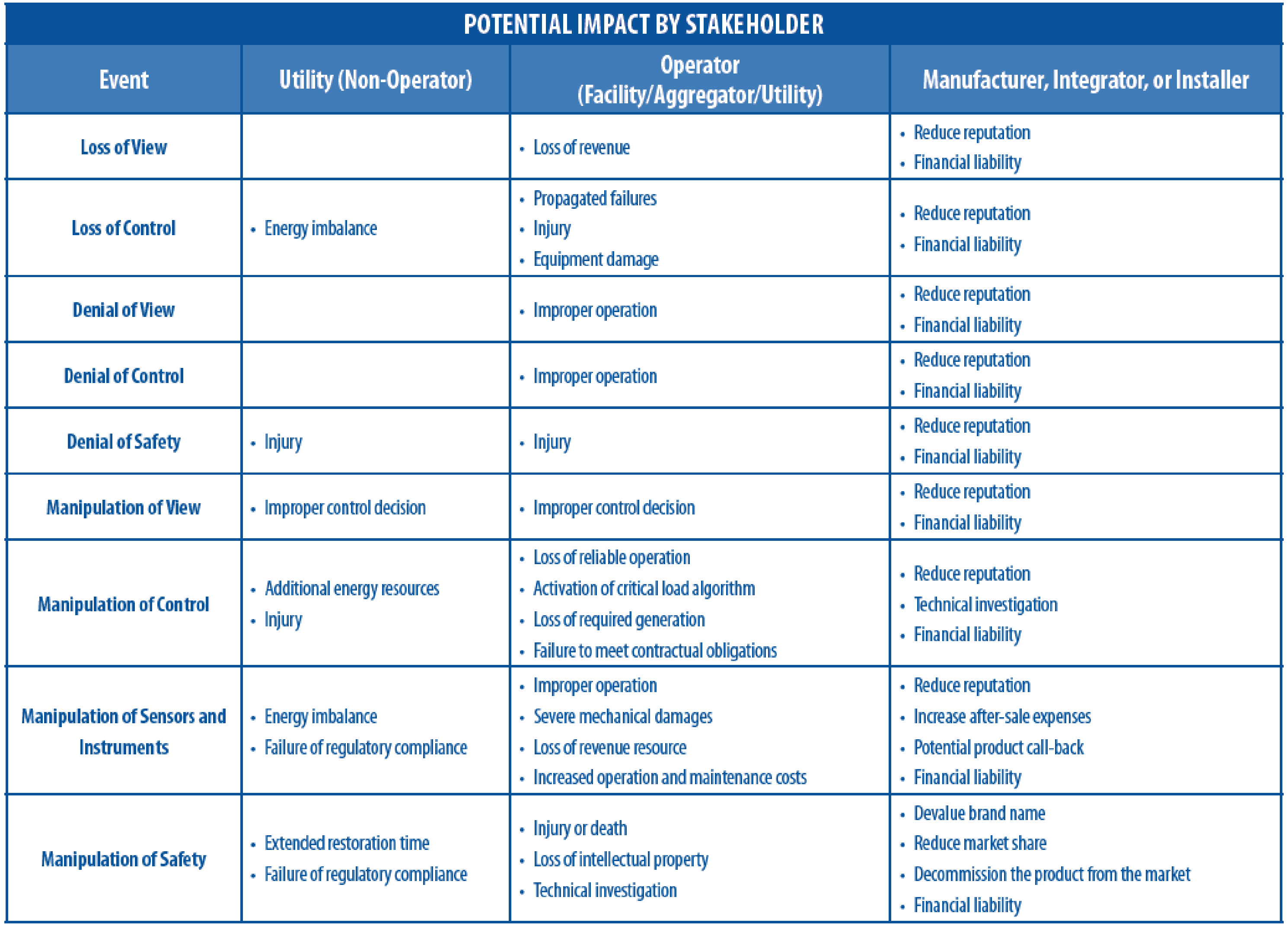
Vulnerability

- **Definition:** a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system
- May be a flaw in either design or implementation
- Can occur at any layer of the system



Cyber Resilience

Impact



POTENTIAL IMPACT BY STAKEHOLDER			
Event	**Utility (Non-Operator)**	**Operator (Facility/Aggregator/Utility)**	**Manufacturer, Integrator, or Installer**
Loss of View		• Loss of revenue	• Reduce reputation • Financial liability
Loss of Control	• Energy imbalance	• Propagated failures • Injury • Equipment damage	• Reduce reputation • Financial liability
Denial of View		• Improper operation	• Reduce reputation • Financial liability
Denial of Control		• Improper operation	• Reduce reputation • Financial liability
Denial of Safety	• Injury	• Injury	• Reduce reputation • Financial liability
Manipulation of View	• Improper control decision	• Improper control decision	• Reduce reputation • Financial liability
Manipulation of Control	• Additional energy resources • Injury	• Loss of reliable operation • Activation of critical load algorithm • Loss of required generation • Failure to meet contractual obligations	• Reduce reputation • Technical investigation • Financial liability
Manipulation of Sensors and Instruments	• Energy imbalance • Failure of regulatory compliance	• Improper operation • Severe mechanical damages • Loss of revenue resource • Increased operation and maintenance costs	• Reduce reputation • Increase after-sale expenses • Potential product call-back • Financial liability
Manipulation of Safety	• Extended restoration time • Failure of regulatory compliance	• Injury or death • Loss of intellectual property • Technical investigation	• Devalue brand name • Reduce market share • Decommission the product from the market • Financial liability

Cyber Resilience

Cyber Resilience by Design

- Resilience measures can be applied to any component of risk
- Build layered protections to achieve defense-in-depth for critical assets, processes, and services
- Evaluate cyber risk regularly
- Ensure lifecycle management occurs
- Risk transfer is also a mitigation

Considerations for Distribution Systems

- Knowledge and tools exist for securing distributed control systems
- Sheer number of digital endpoints pose a challenge
- Fewer regulatory drivers
- Greater diversity of manufacturers increases supply chain risk
- IIJA bill requiring DOE to report on cybersecurity of distribution systems

Key Resources

- U.S. Government Accountability Office: Electricity Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems
- Infrastructure Investment and Jobs Act
- NREL: States of Cybersecurity: Electricity Distribution System Discussions
- Joint INL & NREL report coming soon re: IIJA
- INL: Consequence-driven Cyber-informed Engineering (CCE)
- DOE CESER: National Cyber-Informed Engineering Strategy (CIE)
- Canadian Centre for Cyber Security: National Cyber Security Strategy
- U.S. and Canada: Joint United States-Canada Electric Grid Security and Resilience Strategy (2016)
- INL: Cyber-Resilience Risk Management Architecture

References

- https://www.wsj.com/articles/european-wind-energy-sector-hit-in-wave-of-hacks-11650879000
- https://renewablesnow.com/news/disrupted-satellite-connection-hits-5800-enercon-turbines-report-775234/
- https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/
- https://www.vestas.com/en/media/company-news/2021/third-update-on-cyber-incident-c3466518
- https://www.deutsche-windtechnik.com/press-information/item/463-Cyber-attack-on-Deutsche-Windtechnik
- https://securityboulevard.com/2022/05/cyber-attacks-on-the-power-grid/
- https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/
- https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns
- https://www.recordedfuture.com/redecho-targeting-indian-power-sector
- https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets
- https://www.govtech.com/sponsored/back-to-basics-a-deeper-look-at-the-colonial-pipeline-hack
- https://www.verizon.com/business/resources/reports/dbir/

References

- https://www.dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/
- https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector
- https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
- https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
- https://www.cbc.ca/news/canada/north/ntpc-apparent-ransomware-attack-1.5551603
- https://www.wired.com/story/iran-hackers-us-phishing-tensions/
- https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new
- https://www.wired.com/story/triton-hackers-scan-us-power-grid/
- https://us-cert.cisa.gov/ncas/alerts/TA18-074A
- https://www.cbc.ca/news/technology/hackers-infrastructure-1.3376342
- https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/
- https://morningconsult.com/2020/08/27/cyber-attacks-gas-electric-utilities-data/

Thank You

Megan Culler
Idaho National Laboratory
Critical Infrastructure Security
Megan.Culler@inl.gov