This briefing was developed for **The Blue Book Project**, lead by the Commonwealth of Virginia, support by CNA, and funded through a FEMA regional catastrophic planning grant.

Blue Book Project Goal: Develop a coordinated operational process to support local, state, federal, and private sector priorities; support Virginia residents; and ensure continuity of government while managing consequences from a coordinated nation-state cyberattack on critical lifeline services.

The Blue Book Project

The Blue Book Project

Cyberattack Threat Briefing

“Cyberattack” is a very broad term

Cyberattack: “Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain”

--Committee on National Security Systems Instruction (CNSSI) 4009

The Blue Book Project

Cyberattacks come in many forms

The following are examples of who perpetrates them, how they are conducted, and what form the attack takes.

Who:

- Nation states
- Criminal enterprises
- Private companies, working with government
- Hacking groups, loosely aligned with a state
- Individuals

How:

- Internet connection
- Radio frequency connection
- Insider threat
- Unwitting insider
- Supply chain

What:

- Custom malware
- Malware as a service
- Living off the land attacks
- Sophisticated and surgical
- Brute force and indiscriminate

The Blue Book Project

Cyberattacks are appealing to adversaries

- Nations can avoid all-out military conflict
- Attackers can deny responsibility, if desired
- Cyber weapons or effects can be “pre-positioned”
- Many poorly defended critical infrastructure sites
- Cyberattacks can have enormous impact
- For example:

CHANGE HEALTHCARE

2024, payment disruptions

Colonial Pipeline Company

2021, fuel supply disruptions

The Blue Book Project

"OT" is where cyber becomes physical

Information technology (IT)

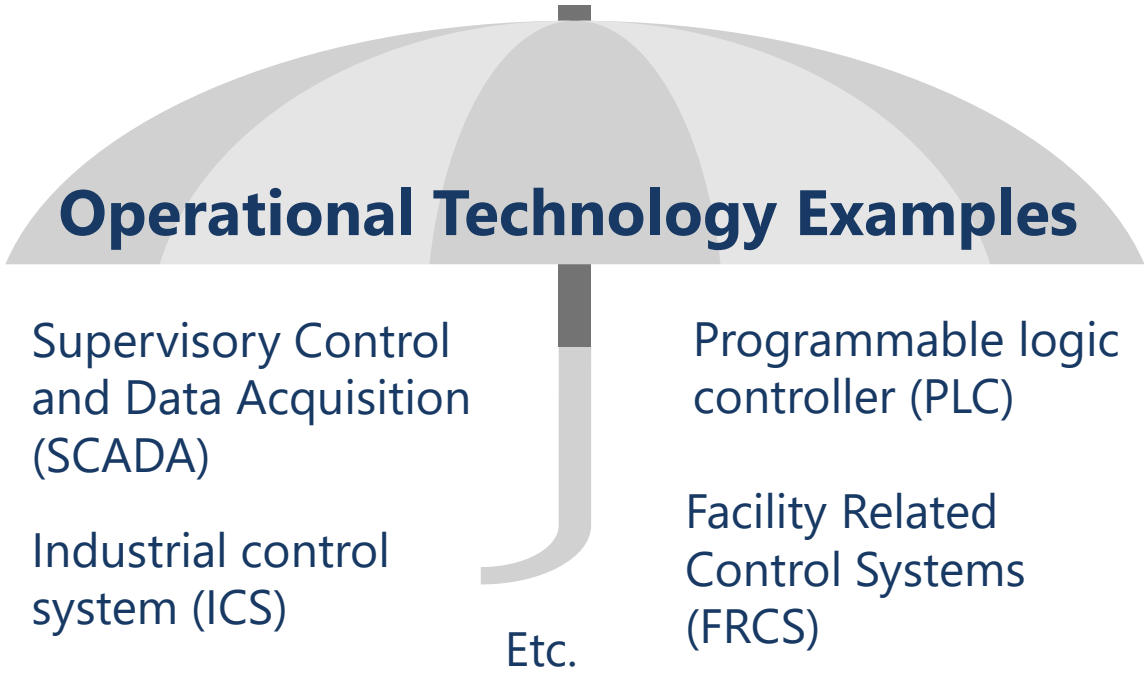
Systems that process, exchange, store, etc. information and data

- e.g., corporate network

Operational Technology (OT)

Systems or devices that interact with the physical environment

- e.g., remotely operated valve



The Blue Book Project

Successful OT attacks could have serious cascading effects

An OT cyberattack could cause more damage than common equipment failures or natural disasters.

A thinking adversary could…

- Target hard-to-repair components
- Cause cascading failures
- Combine OT and IT attacks
- Combine false and misleading information operations to maximize impact

The US has capable competitors

- Cyberattacks are hard to execute, particularly against OT
  - "Air gapped," complex systems, require technical expertise
- But many groups are doing that long, hard work
  - Volt Typhoon – years of presence on critical infrastructure
  - xz Utils attack – years long, supply chain effort
- Competitors have large military and civilian cyber forces as well as relationships with non-government actors
- Competitors and adversaries have had many years and many people to develop threats to Virginia's critical infrastructure

The Blue Book Project

Three things to leave this briefing with…

- A cyberattack on our critical infrastructure could have effects that are widespread, be difficult to recover from, and put lives at risk.
- Adversaries and competitors have had many years to develop cyberattack capabilities, many people to do it, and many critical infrastructure targets to choose from.
- The United States has not yet seen a ‘really bad day,’ but it is technically possible and there are adversaries who are actively working towards it.

Let's Connect

Feel free to email us with questions

bluebookproject@vdem.virginia.gov

Check out the Blue Book TV Reading Corner for more information and resources

Reading Corner - The Blue Book Project | VDEM

The Blue Book Project