CYBERSECURITY & THE PNW POWER GRID

Birol Yeşilada & Tuğrul Daim

Mark O. Hatfield Cybersecurity and Cyber Defense Policy Center of PSU

Founding partner of

Oregon Cybersecurity Center of Excellence

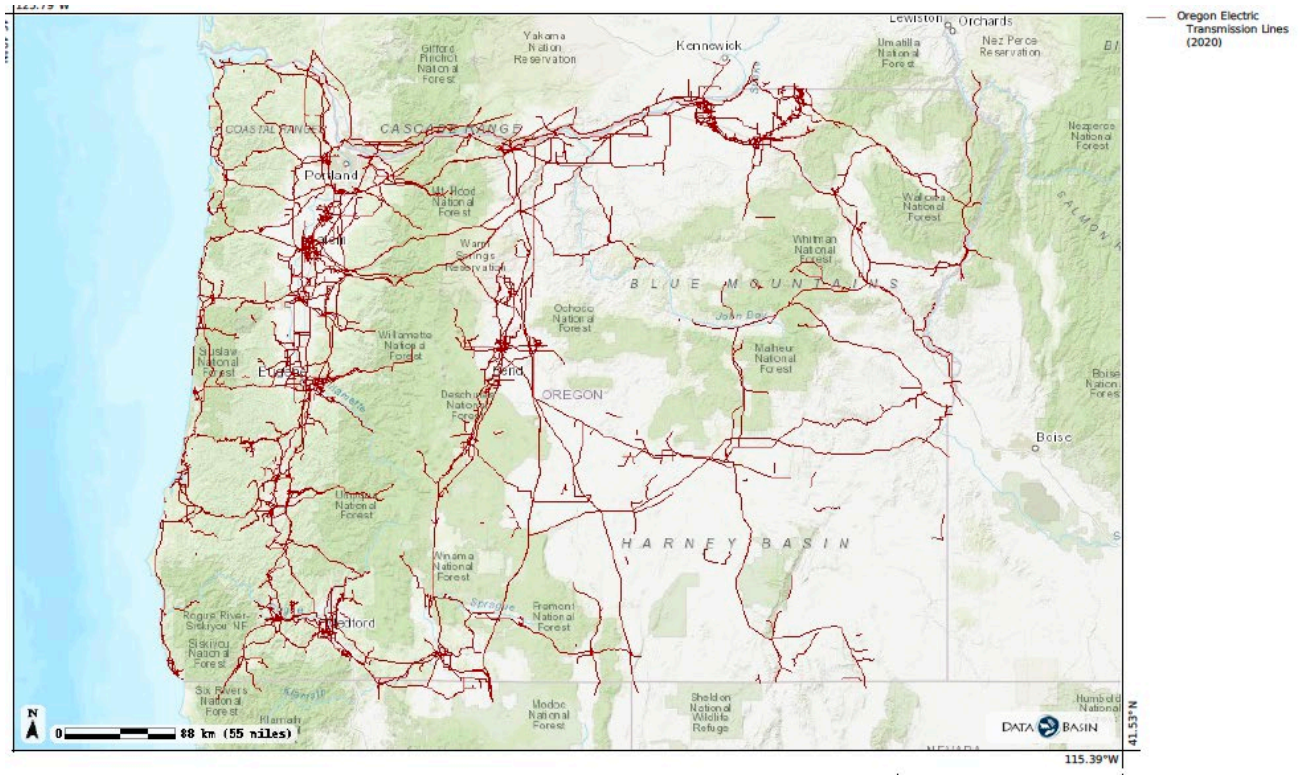
Oregon's Power Grid

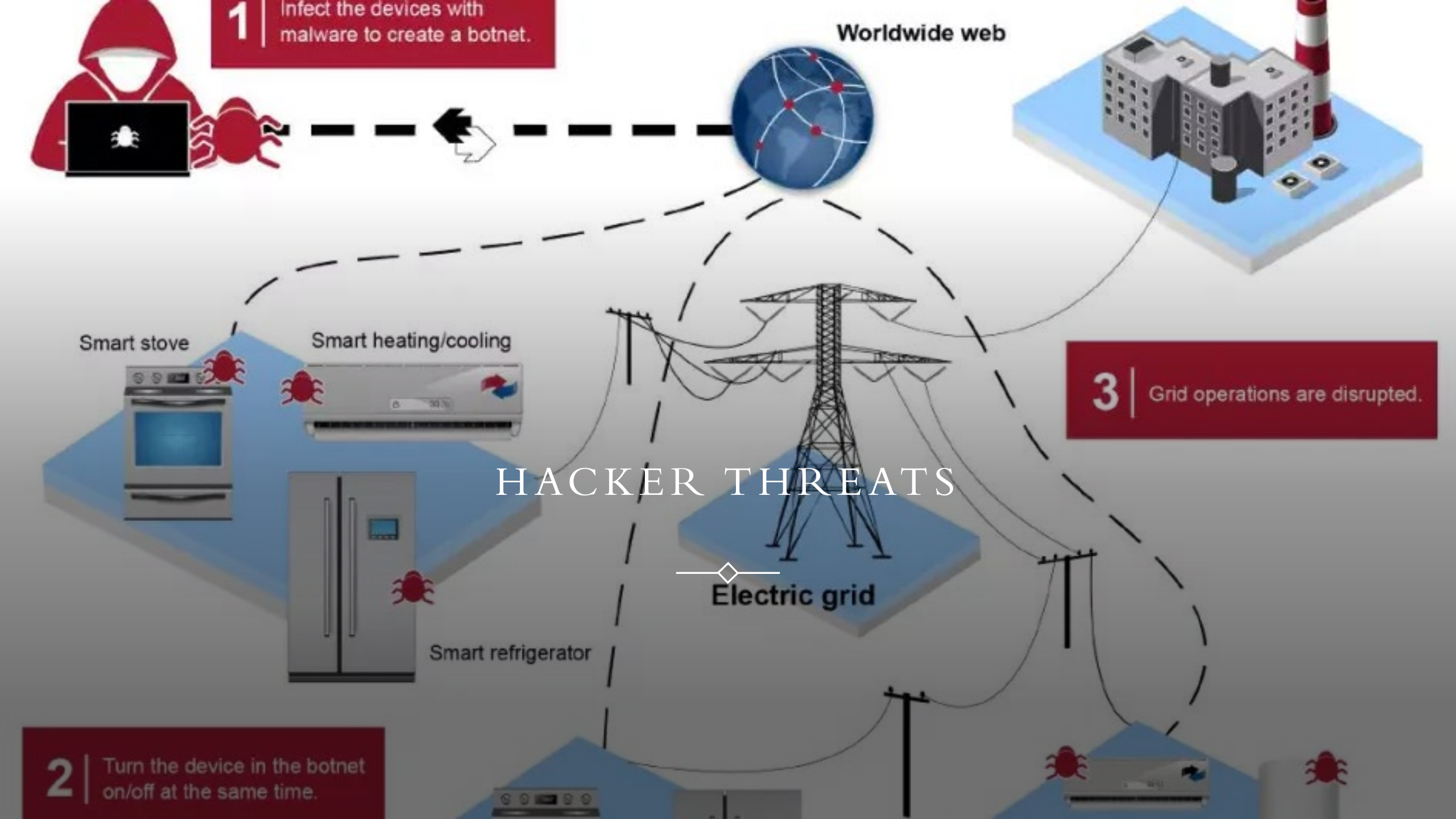
Investor-owned utilities

Portland General Electric (PGE), Pacific Power, and Idaho Power, while the natural gas IOUs consist of NW Natural, Avista, and Cascade Natural Gas.

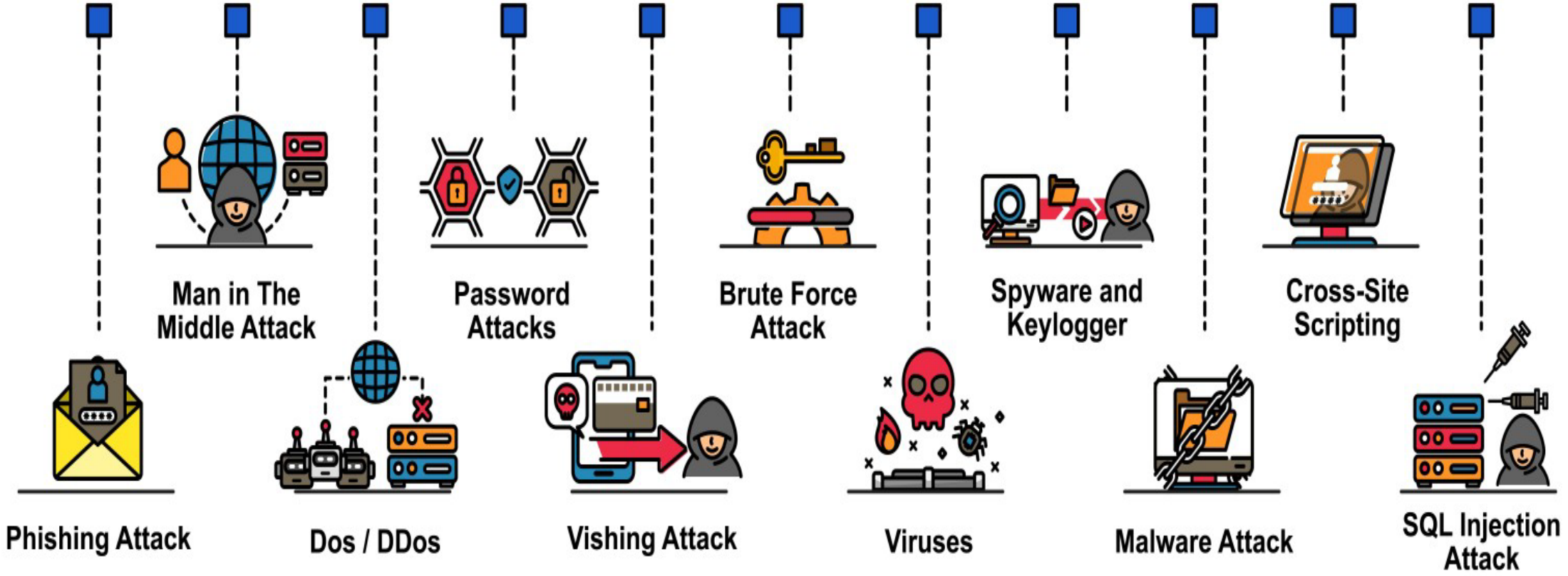
Consumer-owned utilities (n=36)

Cooperatives, Municipal utilities, and

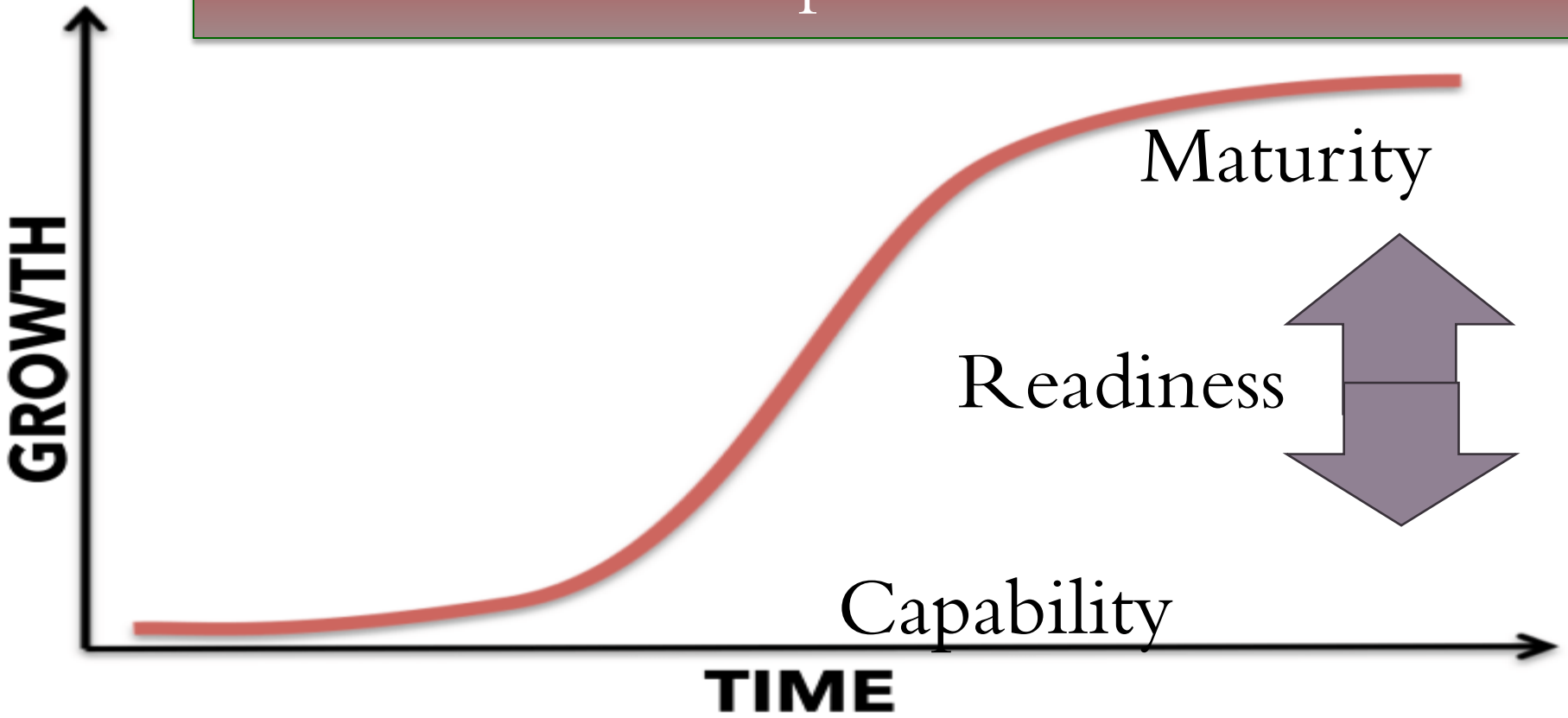



1 Infect the devices with malware to create a botnet.
Worldwide web
Smart stove
Smart heating/cooling
3 Grid operations are disrupted.
HACKER THREATS
Electric grid
Smart refrigerator
2 Turn the device in the botnet on/off at the same time.

CYBER SECURITY ATTACKS



NW Power Grid Cybersecurity Technology Roadmap: Ransomware



Gap Analysis | Methodology | Research Model | Application | Conclusion

Technology Roadmap

- Technology Road mapping (TRM) is a path forward considering current and anticipating future needs and technology capabilities.
- Technology Road mapping is a strategic method of R&D planning.
- Technology roadmaps ensure that investment in technology and research is connected to important industries and the public, and they provide a framework for future breakthroughs and initiatives across multiple disaster technology fields.
- The resulting roadmap is a 221-page document, detailing the critical gaps, potential solutions and R&D Programs . NIST’s Cybersecurity Framework was adopted for the roadmap.

Serious Concerns Requiring Immediate Action*

- Aging Infrastructure
- Smart grid integrations
  - Rural to urban connectivity, broadband, and smart cities
- Substation vulnerabilities
- Cybersecurity skill gap
- Social engineering
- **Fragmented Cybersecurity Policies**
- Foreign enemies of the United States (each has particular approach to information warfare and cyber warfare)
- China, Russia, North Korea, and Iran (in particular).

*Details can be discussed in a CUI setting

China

- The Chinese have stolen classified data on most, if not all, nuclear and neutron bombs in the U.S. arsenal, as well as missile guidance systems.
- Massive Espionage tactics using cyber capabilities
- China is behind a newly discovered series of hacks against key targets in the U.S. government, private companies, and the country's critical infrastructure
- The Chinese have been busy mapping and tapping (with spyware and malware) the **electrical grid** of the United States, various critical infrastructures, including telephone switches, computer networks, electrical systems, emergency management frameworks, transportation networks, banking and financial systems, and governmental structures.
- All of this is part of the Chinese warfare strategy to create disruptions and chaos in the U.S. before the invasion of Taiwan.

RUSSIA

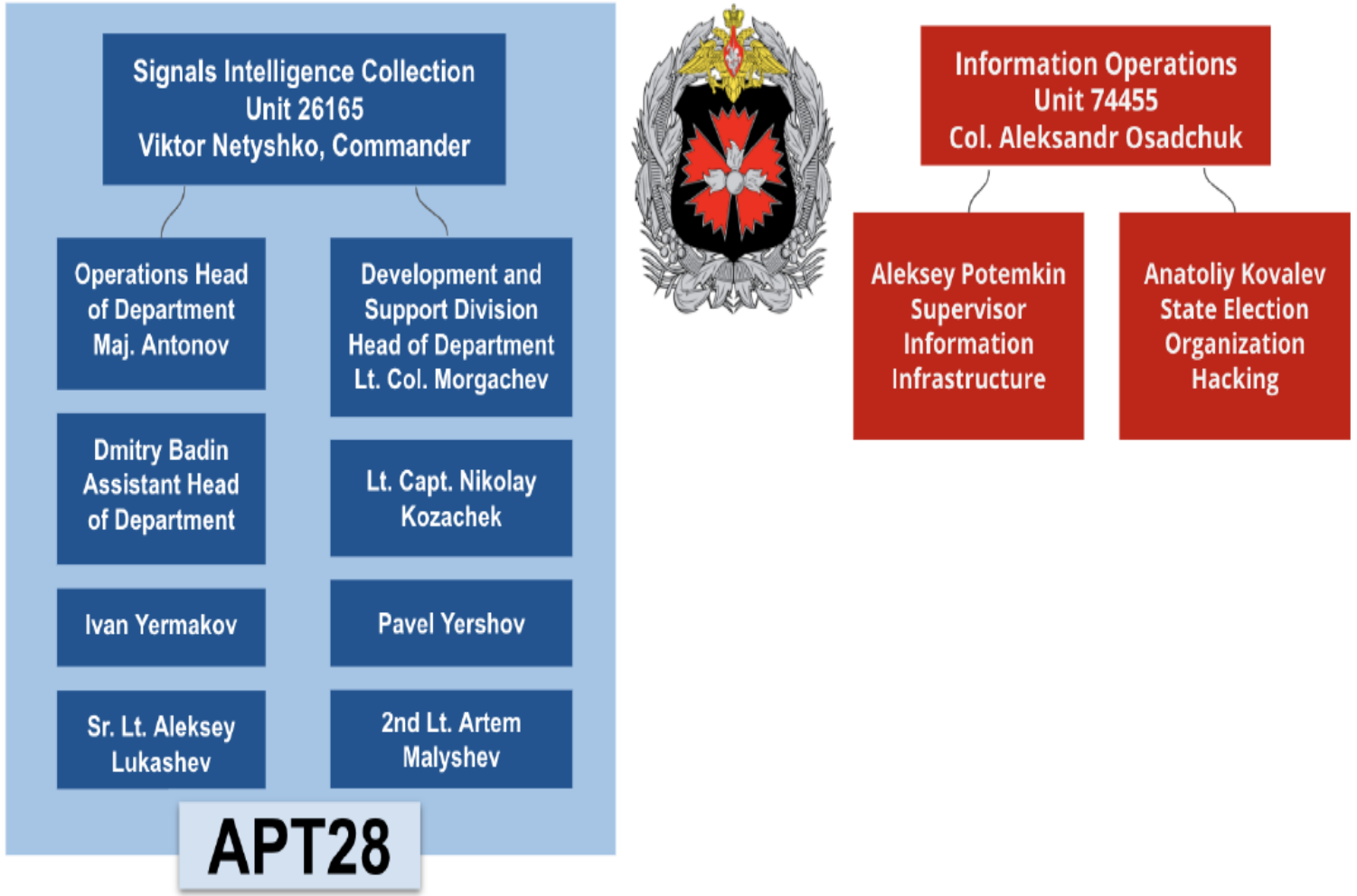
Vladimir Putin's Russia was perhaps first among major powers to deploy techniques of full-spectrum, state-sponsored disinformation for the digital age—the intentional spread of inaccurate information designed to influence societies.

1. Disruption
2. Distortion
3. Deterioration
4. Create mistrust of governments

DISMANTLE DEMOCRACIES FROM WITHIN

SECOND: frontal attacks (Estonia, NATO, Georgia, Crimea, Ukraine)

GRU/GU Units and Staff Involved in 2016 Election Interference



Remedies

- Develop multi-disciplinary technologies to leverage cyber-physical information to defend systems against cyberattacks. The related research questions are:
- Identify key points to monitor network traffic for threat identification
- Use cyber-physical dependency information to determine potential impacts and isolation strategies
- **PROTECT**: Information Protection Processes and have capability gaps.
- **DETECT**: Continuous Security Monitoring is the area with]capability gaps.
- **RESPOND**: Communications is the area with serious capability gaps.
- **RECOVER**: Identify Asset Management shows capability gaps.
- **Immediate attention should be given to**
  - *Identification of cyber-physical interdependency to detect, isolate, and mitigate ransomware attacks*
  - *Design and develop OT-specific threat visualization, intrusion and anomaly detection and mitigation algorithms*
  - *Distributed Oversights Based on Physics-Based Modeling and Observation Against Cyber Manipulation*
  - *Adoption of Artificial Intelligence in a rational manner.*

The benefits of automating AI in cybersecurity:

Ongoing learning

Discovering unknown threats

Vast data volumes

Improved vulnerability management

Enhanced overall security posture

Better detection and response

Negative implications

•**AI-Powered Attacks:** Cybercriminals can also use AI to create more sophisticated and targeted attacks. For example, AI can be used to generate convincing phishing emails, create malware that can evade detection, and automate attacks at scale.

•**Data Poisoning:** Attackers can manipulate the data used to train AI security systems, causing them to make incorrect decisions or miss threats.

•**Bias and Discrimination:** AI systems can inherit biases from the data they are trained on, which can lead to unfair targeting or discrimination.

•**Lack of Transparency:** The decision-making processes of some AI systems can be opaque, making it difficult to understand why they made a particular decision. This can raise concerns about accountability and trust.

Overall implications of AI

- AI is a double-edged sword in cybersecurity. It offers significant potential to improve defenses and combat cyber threats, but it also creates new risks and challenges.

- Organizations need to be aware of both the benefits and the risks of AI and take steps to ensure that it is used responsibly and ethically.

Key considerations for organizations

- **Invest in AI-powered security tools:** These tools can help organizations detect and respond to threats more effectively.
- **Train security personnel on AI:** Security teams need to understand how AI works and how it can be used both for and against them.
- **Address bias and discrimination:** Organizations need to ensure that their AI systems are trained on diverse and representative data to avoid bias.
- **Ensure transparency and accountability:** Organizations should strive to understand how their AI systems make decisions and be able to explain those decisions to others.
- **Stay up-to-date on the latest AI risks:** The field of AI is constantly evolving, so organizations need to stay informed about the latest threats and vulnerabilities.

By taking these steps, organizations can harness the power of AI to improve their cybersecurity posture while mitigating risks.

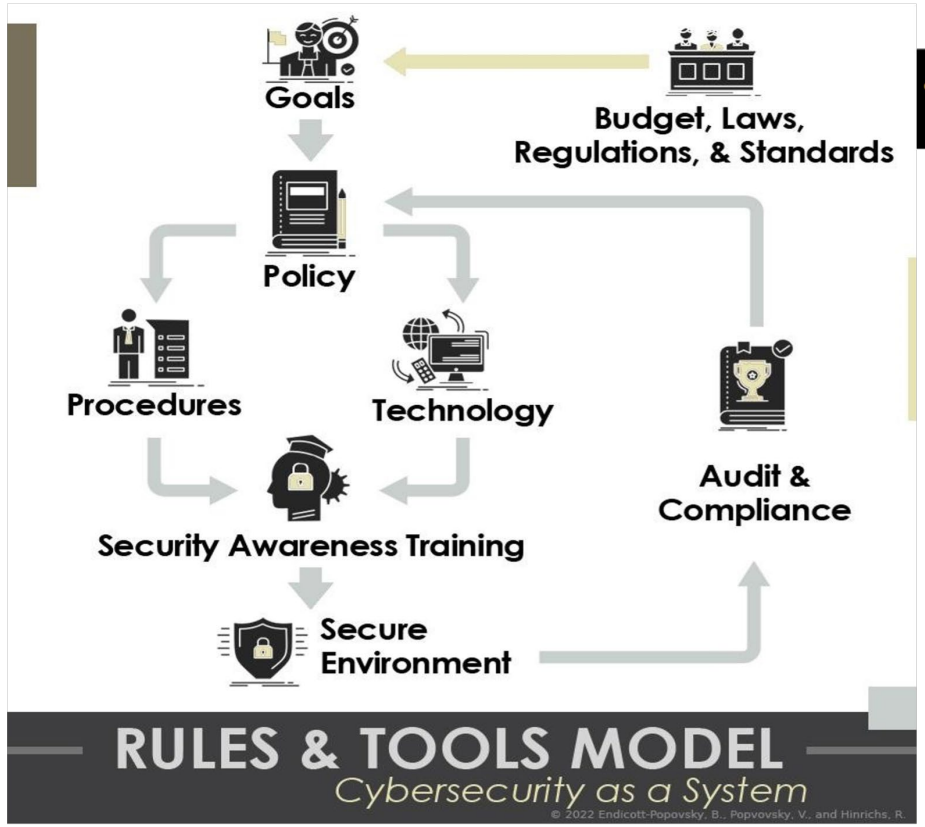
FRAMEWORK

- **Start Here:** The model has a starting point (see finger pointer): Budget, Laws, Regulations & Standards. These flow into defining business goals and imposing compliance-based operational goals for securing the "crown jewels" of any organization.

- **Goals:** To support the requirements imposed by outside bodies (governments, regulatory bodies, international law), each state will have a set of goals to comply with these outside forces.

- **Security Awareness Training.** Cybersecurity rules emerge from local, state, national and federal requirements designed to maintain equilibrium.

- **Auditing and Compliance.** In developing information assurance systems, organizations must consider the interconnectedness of all the different factors that impact them.



Cybersecurity System Model for Engaging each State

Thank you for listening