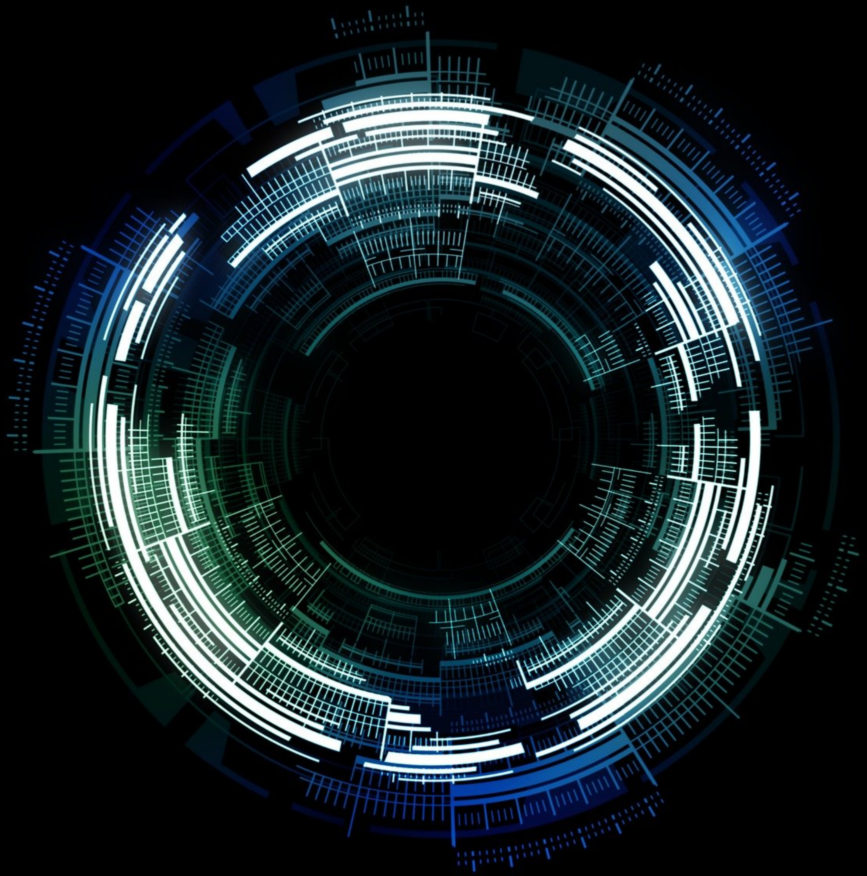


Cybersecurity Analysis of Wind Farm SCADA Systems

2020 International Conference on Information Technologies (InfoTech-2021), IEEE Conference

16-17/09/2021

Cybersecurity Analysis of Wind Farm SCADA Systems

Agenda for today

Topic	**Time**
Industry 4.0 Intro	2 minutes
Wind Turbines Cybersecurity Challenges & Statistics	3 minutes
SCADA wind farm system architecture and possible attacks and attack vectors	5 minutes

Industrial Control Systems (ICS)/SCADA are all around us

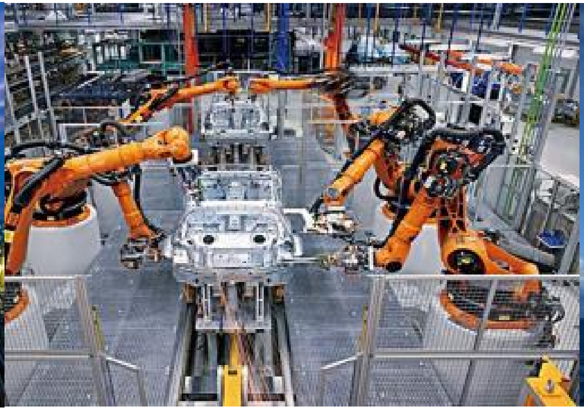
… and we rely on it every day for our basic functions and needs.

Water & Sewage

Electricity

Wind

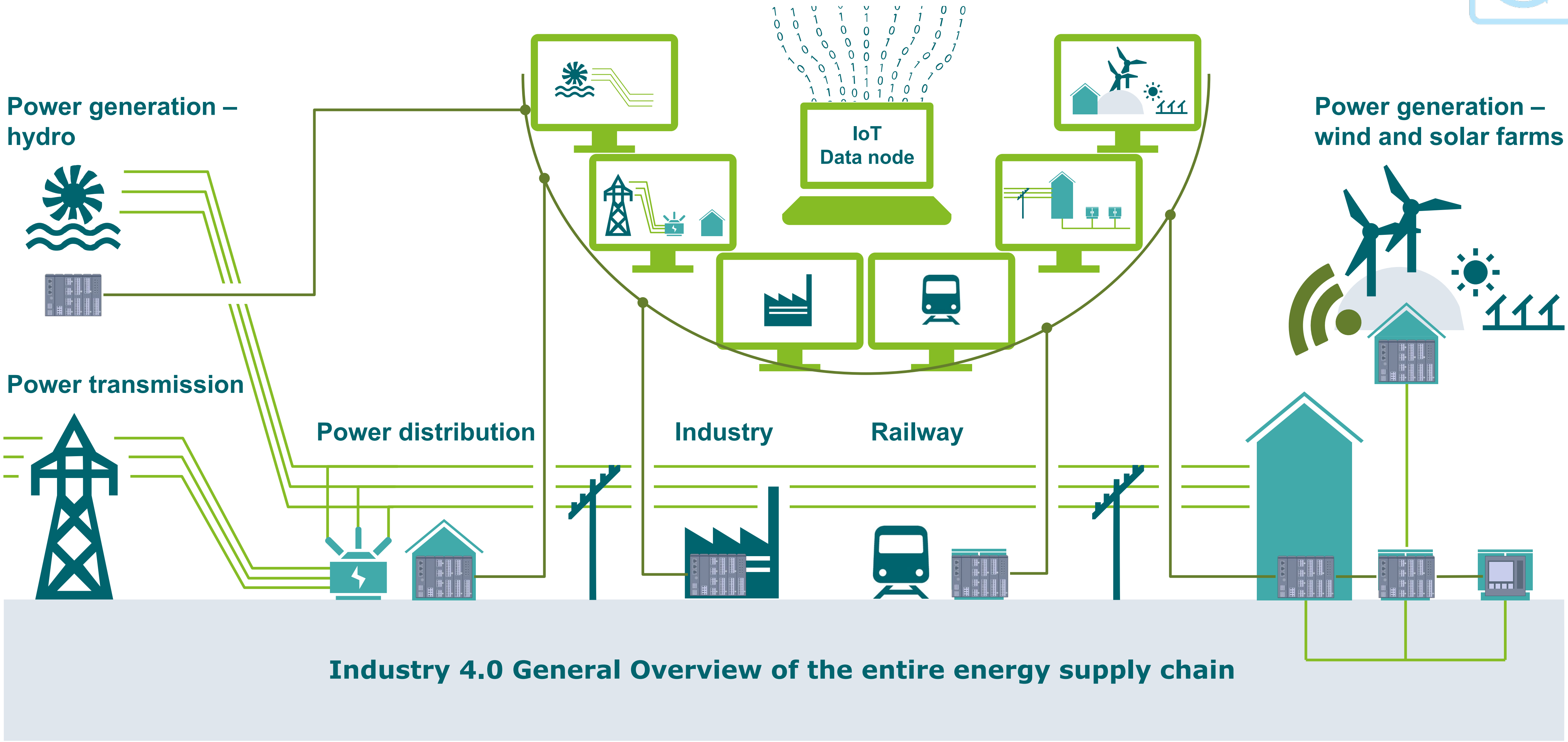
Critical manufacturing



Industrial Automation

Oil & Gas

Industry 4.0 General Overview

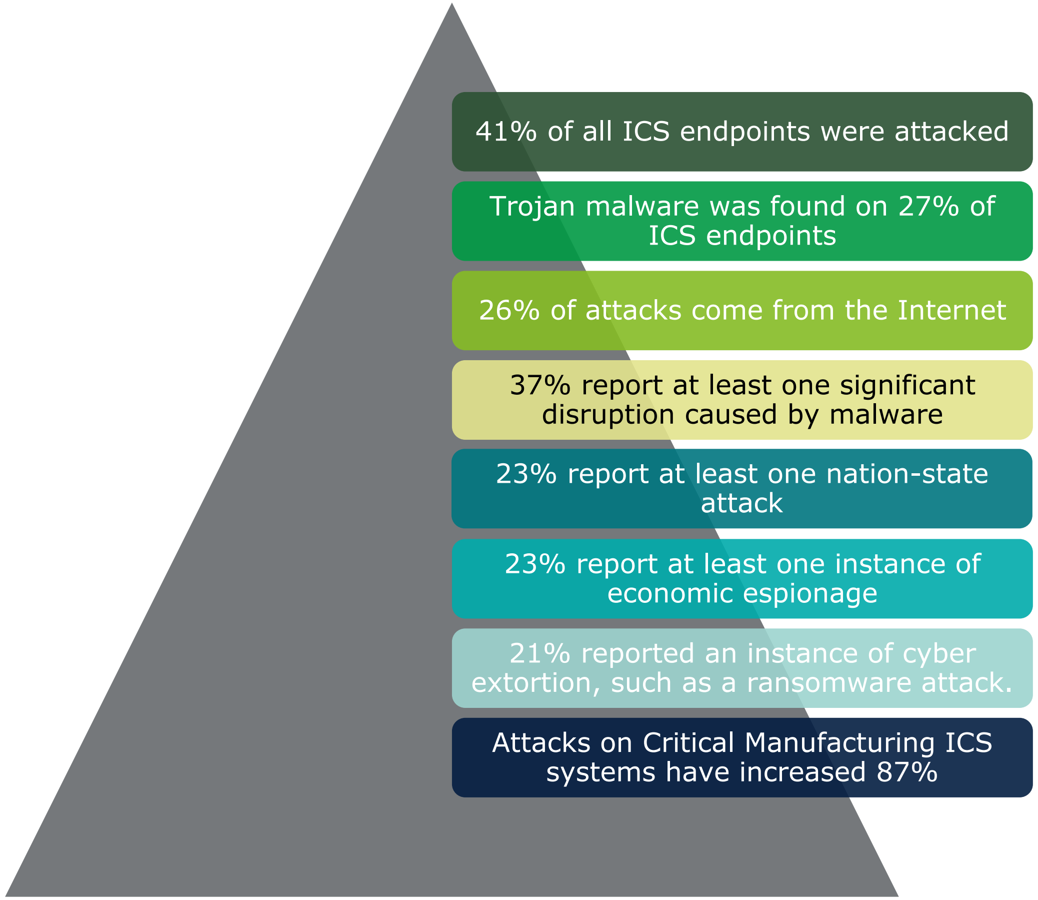


Source https://support.industry.siemens.com/cs/document/109748625/sicam-a8000-cp-8000-cp-8021-cp-8022-package-v12?dti=0&lc=en-AF

Everyone loves statistics

The numbers behind cyberattacks on SCADA are growing

The following building blocks show the statistics behind the growing SCADA/ICS Cyberattacks in the last 12-15 months.



41% of all ICS endpoints were attacked

Trojan malware was found on 27% of ICS endpoints

26% of attacks come from the Internet

37% report at least one significant disruption caused by malware

23% report at least one nation-state attack

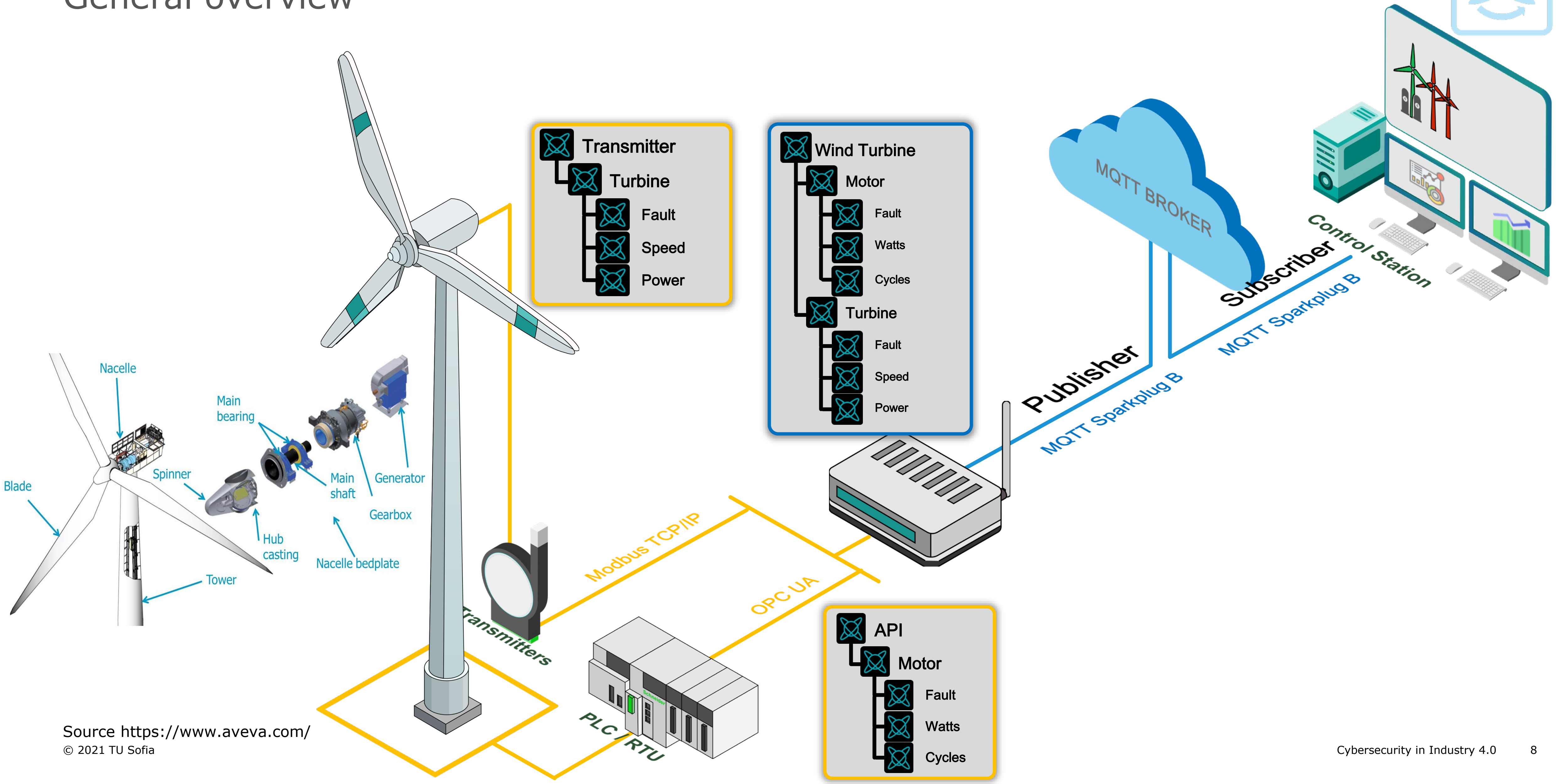
23% report at least one instance of economic espionage

21% reported an instance of cyber extortion, such as a ransomware attack.

Attacks on Critical Manufacturing ICS systems have increased 87%

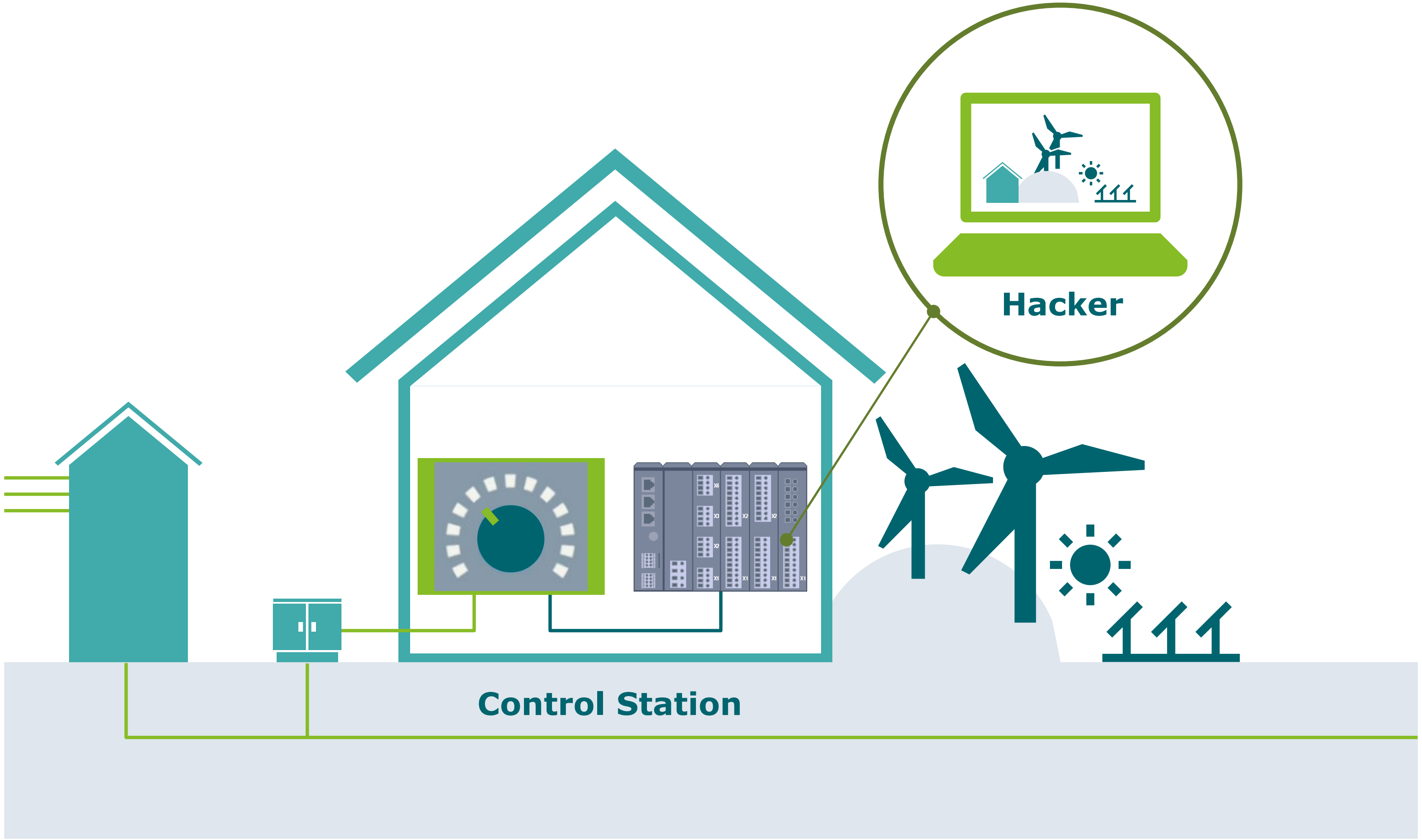
Wind turbines utilizing MQTT

General overview



Source https://www.aveva.com/

SCADA wind farm system architecture and possible attack vectors



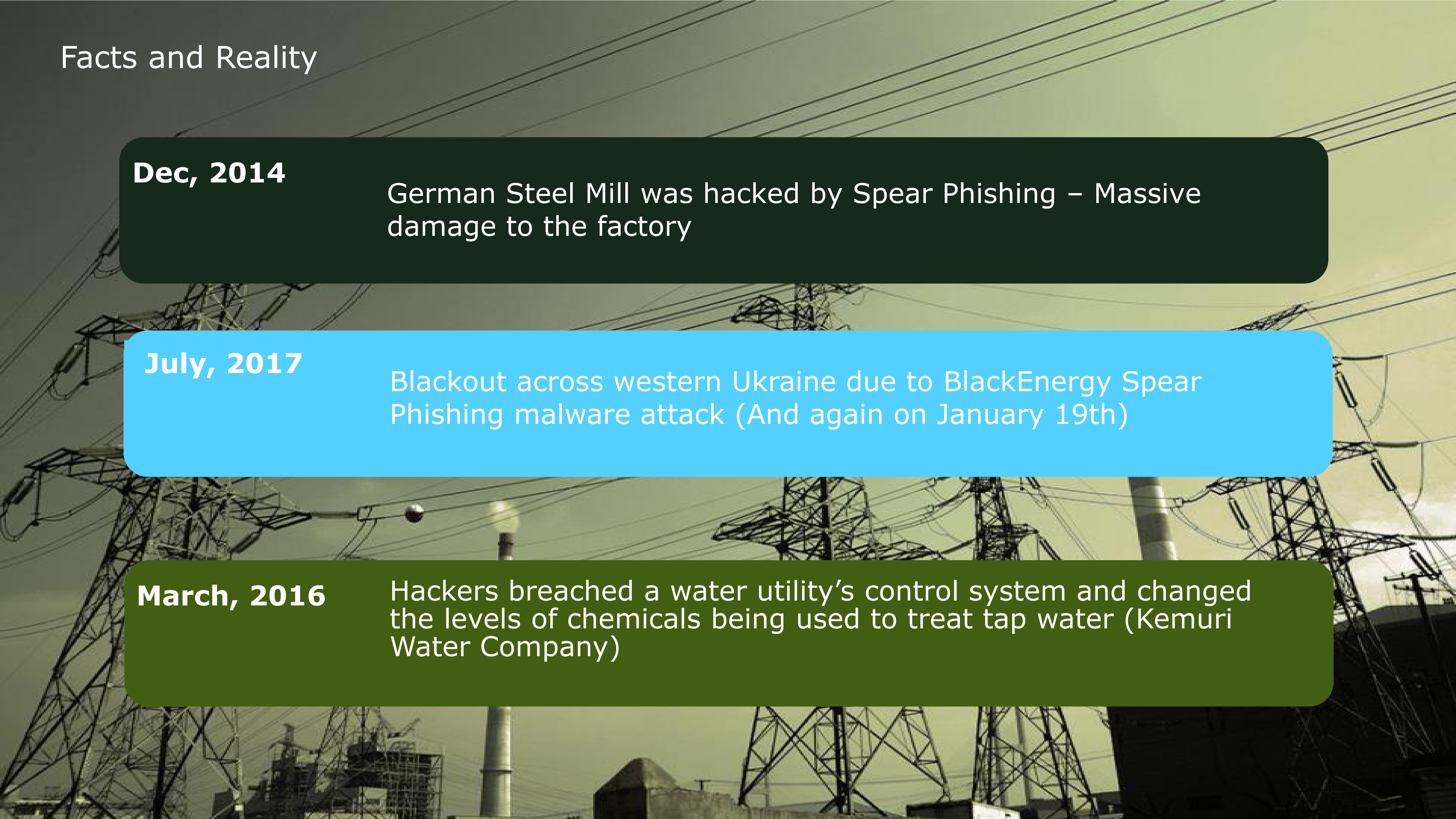
Cyber attacks

Selected attacks are shown below:

- **Physical attack vectors:** Exploits the physical access to the wind turbines. Such kind of attacks have high chances for success
- **Operation continuity vulnerabilities:** Wind farm systems are not prepared to recover and continue its functions if there was a natural disaster such as earthquake, manmade event or even vandalism
- **Network attack vectors:** Wired and Wireless network architectures for wind farms are topic that is being explored by researchers and attackers
- **Human vulnerabilities:** The human beings are prone to errors and often make mistakes

Source https://support.industry.siemens.com/cs/document/109748625/sicam-a8000-cp-8000-cp-8021-cp-8022-package-v12?dti=0&lc=en-AF

Facts and Reality



Dec, 2014

German Steel Mill was hacked by Spear Phishing – Massive damage to the factory

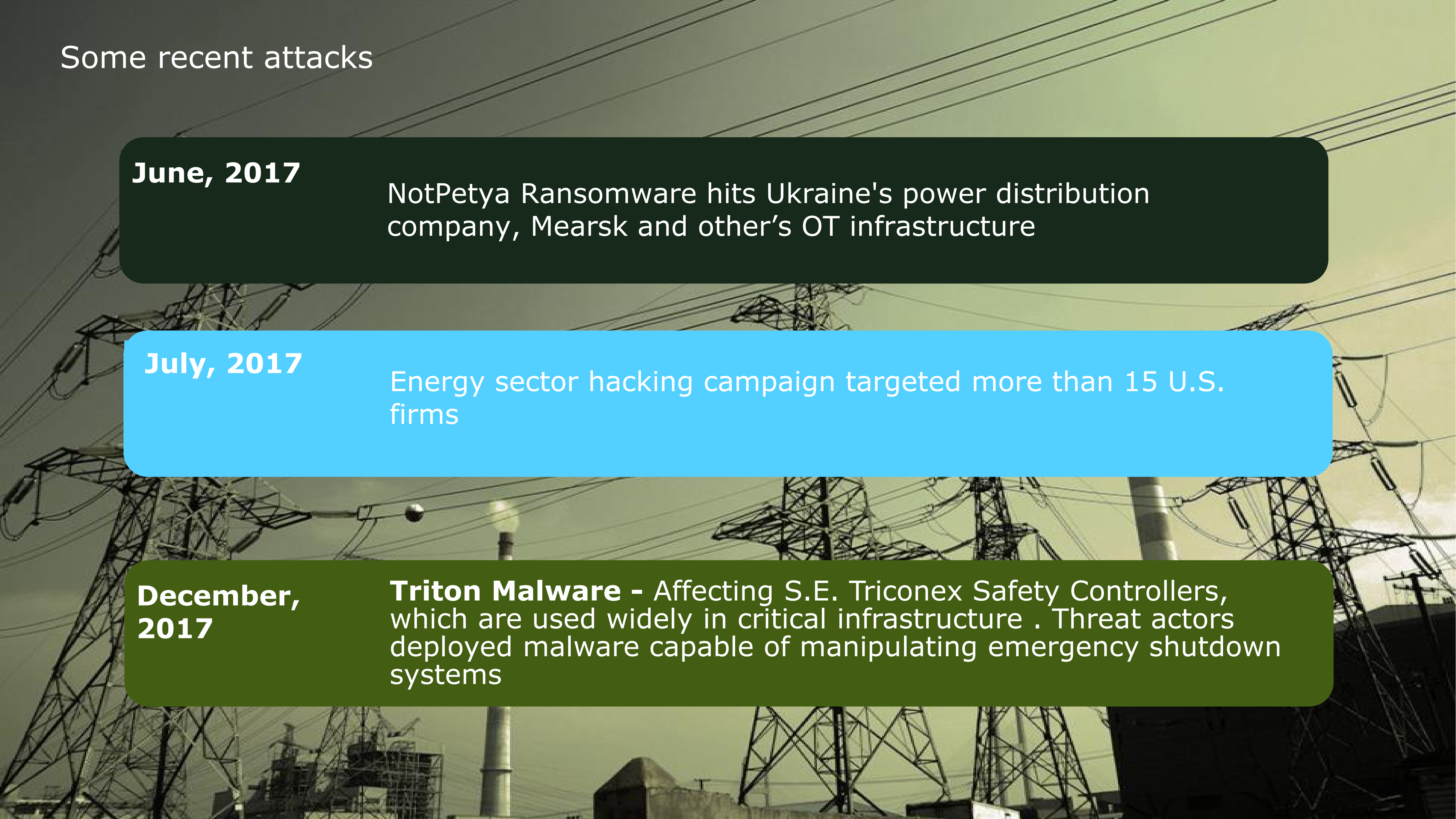
July, 2017

Blackout across western Ukraine due to BlackEnergy Spear Phishing malware attack (And again on January 19th)

March, 2016

Hackers breached a water utility’s control system and changed the levels of chemicals being used to treat tap water (Kemuri Water Company)

Some recent attacks



June, 2017

NotPetya Ransomware hits Ukraine's power distribution company, Mearsk and other’s OT infrastructure

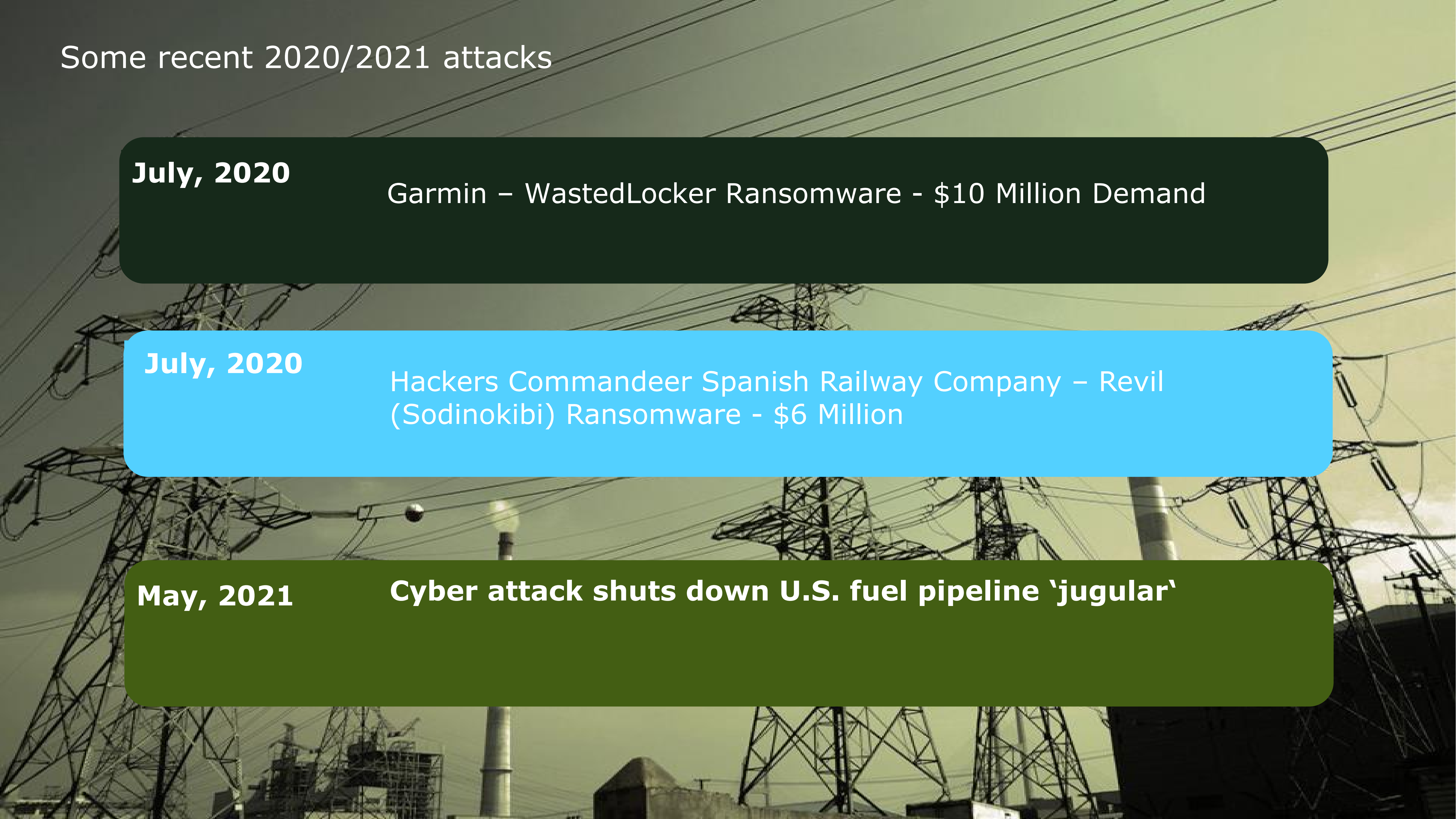
July, 2017

Energy sector hacking campaign targeted more than 15 U.S. firms

December, 2017

Triton Malware - Affecting S.E. Triconex Safety Controllers, which are used widely in critical infrastructure . Threat actors deployed malware capable of manipulating emergency shutdown systems

Some recent 2020/2021 attacks



July, 2020

Garmin – WastedLocker Ransomware - $10 Million Demand

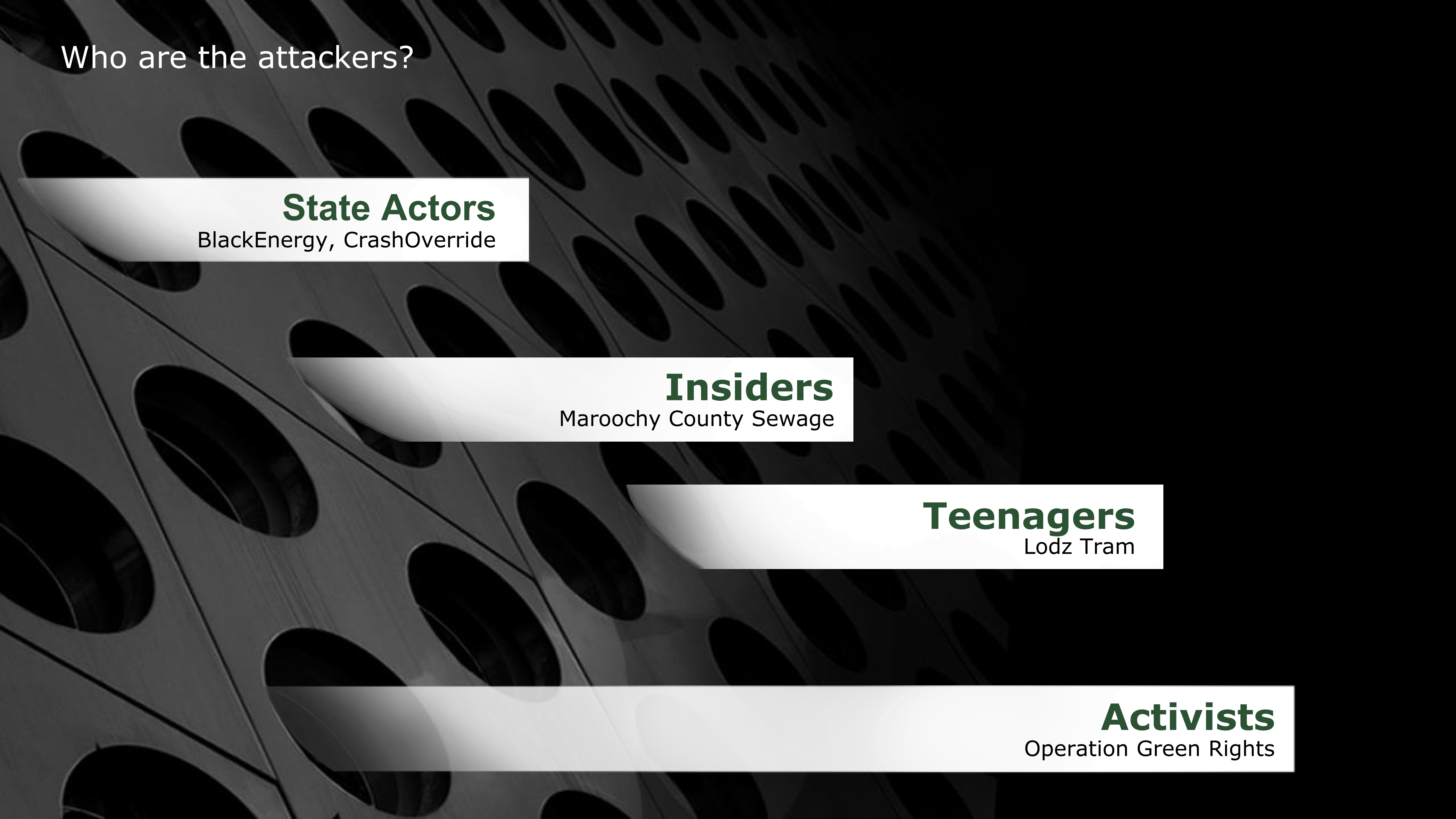
July, 2020

Hackers Commandeer Spanish Railway Company – Revil (Sodinokibi) Ransomware - $6 Million

May, 2021

Cyber attack shuts down U.S. fuel pipeline ‘jugular‘

Who are the attackers?



State Actors
BlackEnergy, CrashOverride

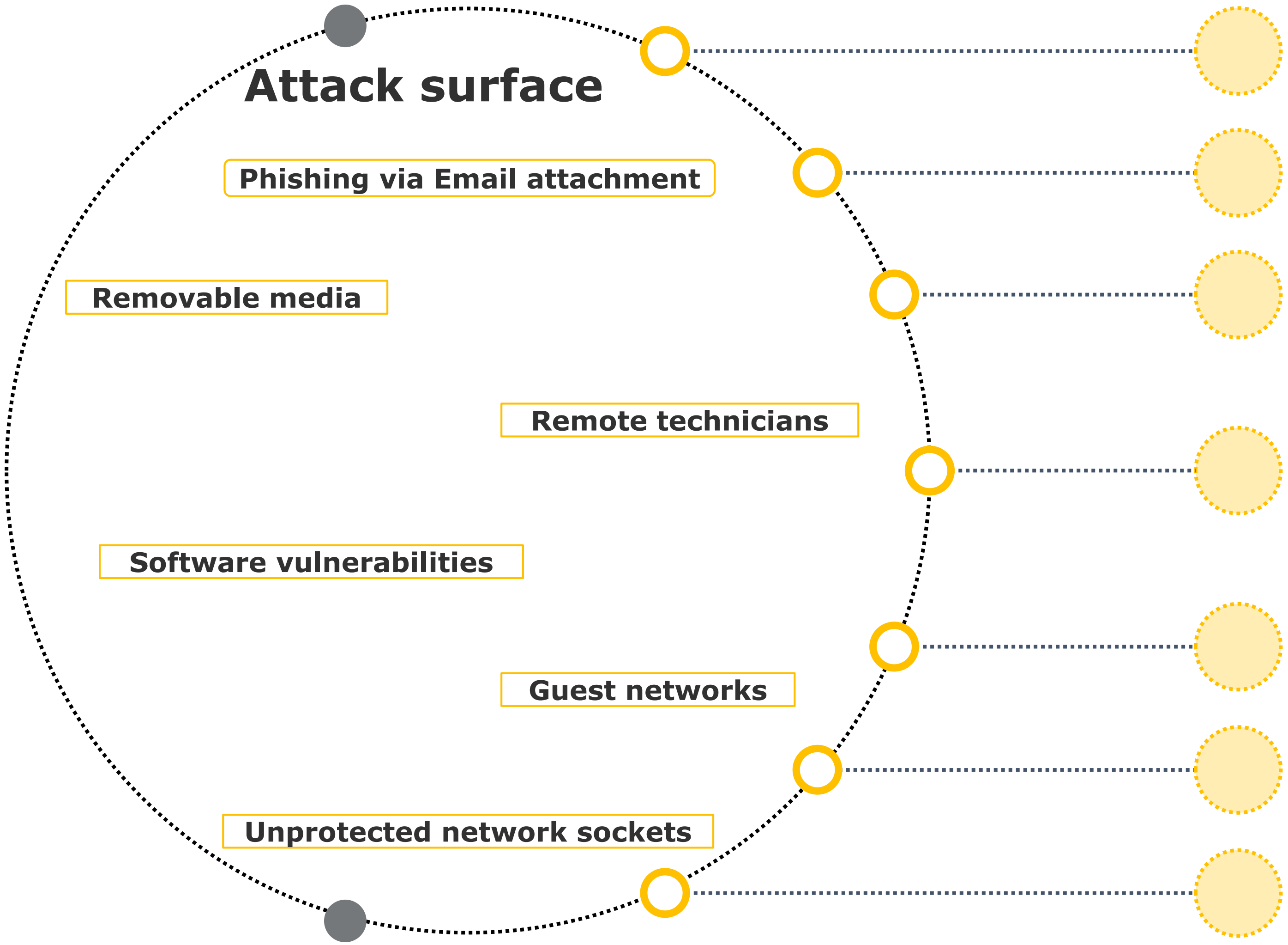
Insiders
Maroochy County Sewage

Teenagers
Lodz Tram

Activists
Operation Green Rights

Why are the attacks possible?

… and what can we do about it.



Attack surface

Phishing via Email attachment

Removable media

Remote technicians

Software vulnerabilities

Guest networks

Unprotected network sockets

Legacy systems

Default configurations

Less/no updates

Less/no encryption

Lack of policies/standards

Less/no segmentation

Latency concerns

Thank you.

Contact information:

Roumen Trifonov
Evgeni Sabev
Galya Pavlova
Kamelia Rainova

Faculty of Computer Systems and Technology
Technical University of Sofia
8 Kliment Ohridski blvd.
1000 Sofia, Bulgaria

r_trifonov@tu-sofia.bg
www.tu-sofia.bg