UNIVERSITY OF Southampton

cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

COMP6224 2019-20
Foundations of Cyber Security

Security of Critical Infrastructure

Week 10 – Tuesday 3rd December 2019

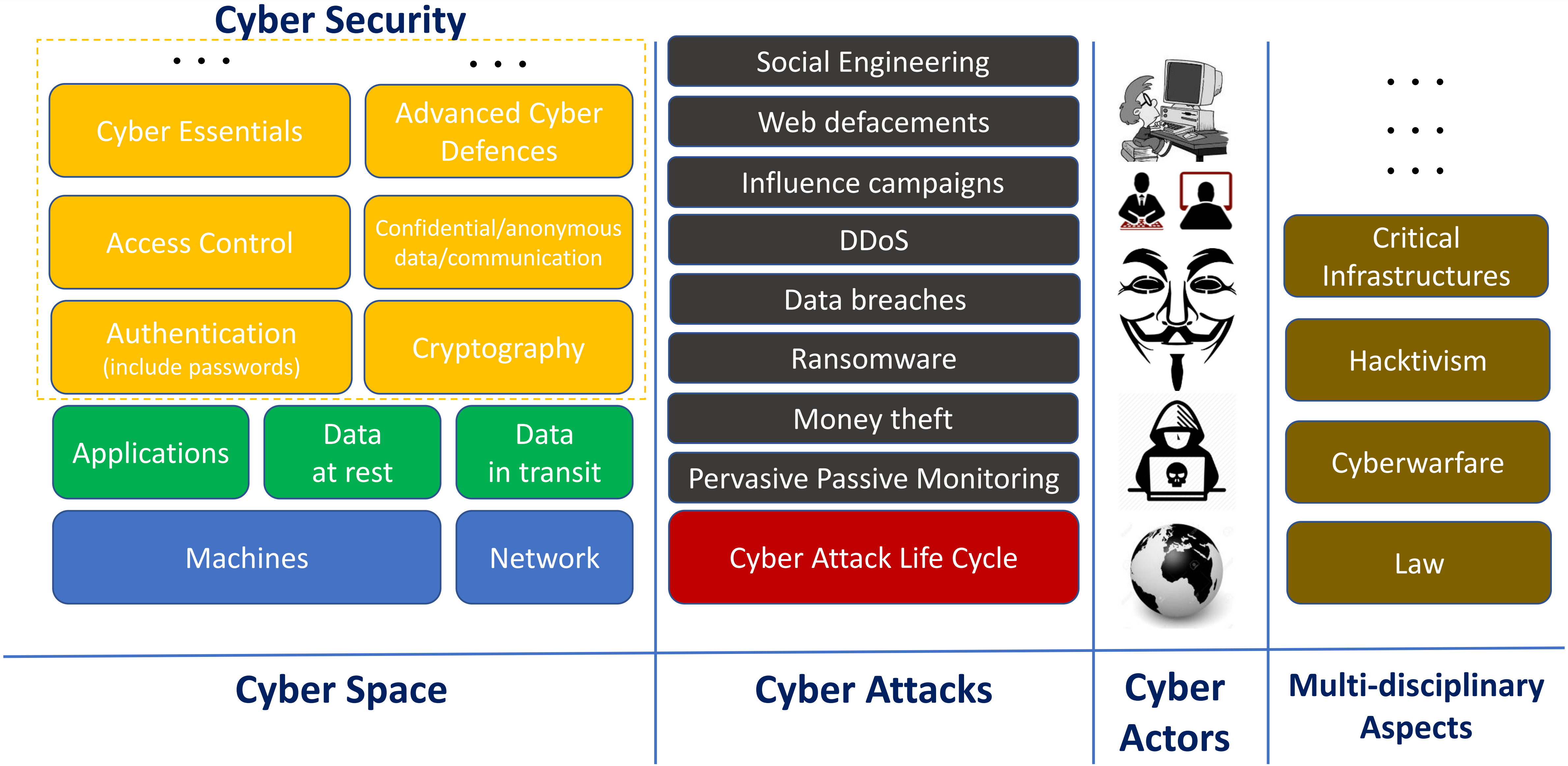
Dr Leonardo Aniello

l.aniello@soton.ac.uk

Cyber Security Research Group

blog | twitter

Link with previous lectures



Cyber Security

. . .

. . .

Cyber Essentials

Advanced Cyber Defences

Access Control

Confidential/anonymous data/communication

Authentication (include passwords)

Cryptography

Applications

Data at rest

Data in transit

Machines

Network

Cyber Space

Social Engineering

Web defacements

Influence campaigns

DDoS

Data breaches

Ransomware

Money theft

Pervasive Passive Monitoring

Cyber Attack Life Cycle

Cyber Attacks

Cyber Actors

. . .

. . .

. . .

Critical Infrastructures

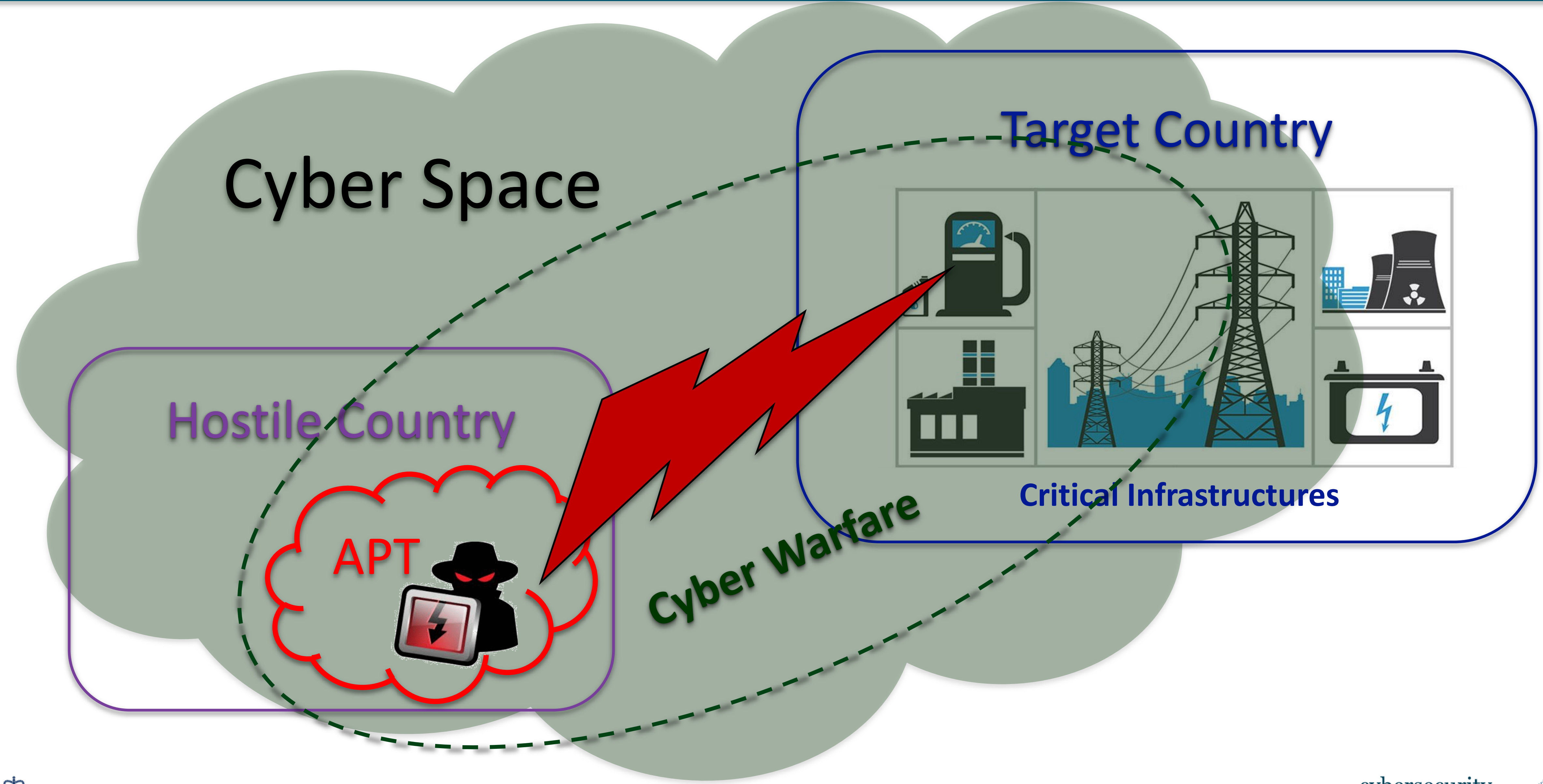
Hacktivism

Cyberwarfare

Law

Multi-disciplinary Aspects

Link with previous lectures



Learning Outcomes

At the end of this lecture you should be able to

- LO1 Recognise societal dependence on Critical Infrastructures and Industrial Control Systems
- LO2 Discuss the cyber security of Industrial Control Systems
- LO3 Understand the anatomy of cyber-attacks against Industrial Control Systems

Outline

- **What is a Critical Infrastructure (CI)?**
- CIs and Industrial Control Systems (ICSs)
- Cyber Security of CIs and ICSs
  - Stuxnet
  - BlackEnergy

What is a Critical Infrastructure (CI)?

- UK Critical National Infrastructure (CNI)

- National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. [Centre for the Protection of National Infrastructure]

What is a Critical Infrastructure (CI)?

- UK National Infrastructure Sectors
  - Chemicals
  - Civil Nuclear
  - Communications
  - Defence
  - Emergency Services
  - Energy
  - Finance
  - Food
  - Government
  - Health
  - Space
  - Transport and Water

Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to ***severe economic or social consequences or to loss of life***

What is a Critical Infrastructure (CI)?

- UK National Cyber Security Strategy 2016-2021
  - Section 5.4: Protecting our Critical National Infrastructure and other Priority Sectors

- Other companies and organisations that require a greater level of support
  - The jewels in our economic crown
  - Data holders
  - High-threat targets
  - The touchstones of our digital economy
  - Organizations influencing the whole economy to improve their cyber security

Outline

- What is a Critical Infrastructure (CI)?

➢ **CIs and Industrial Control Systems (ICSs)**

- Cyber Security of CIs and ICSs
  - Stuxnet
  - BlackEnergy

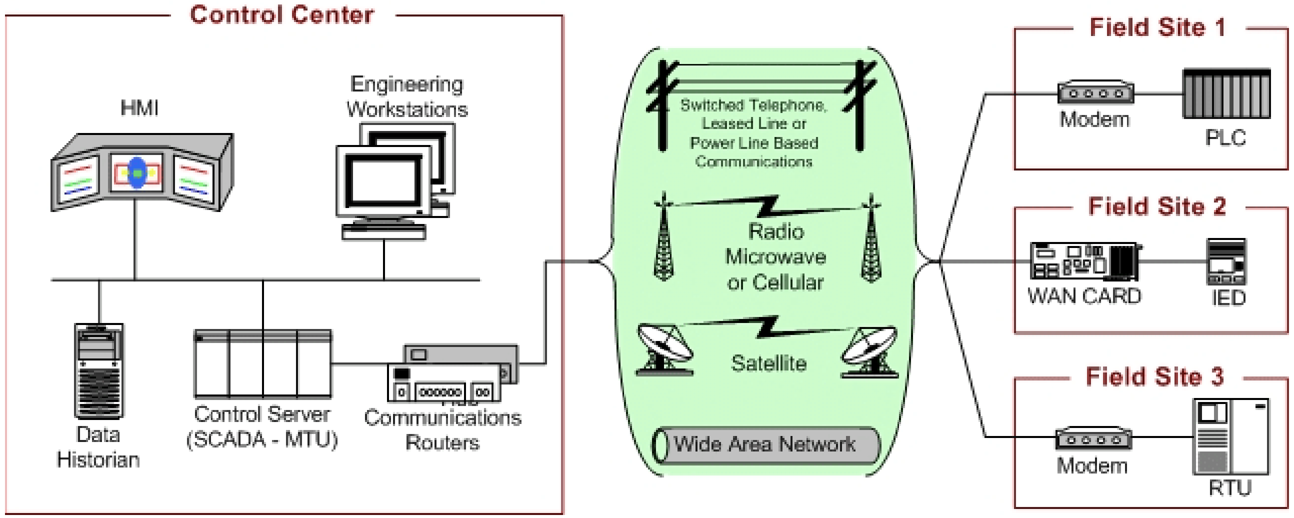
CIs and Industrial Control Systems (ICSs)

- Many CIs are controlled and monitored by Industrial Control Systems (ICS)
    - Electricity generation plants
    - Transportation systems
    - Manufacturing facilities

- “ICS control our critical infrastructures, safety-critical processes and most production processes. ICS are now everywhere around us, often hiding in everyday functionality.” [Luiijf & Paske 2015]

CIs and Industrial Control Systems (ICSs)

- An ICS is made up of
  - Supervisory Control and Data Acquisition (SCADA) systems
  - Remote Terminal Units (RTUs)
  - Master Terminal Units (MTUs)
  - Programmable Logic Controllers (PLCs)
  - Human–Machine Interfaces (HMIs)
  - Intelligent Electronic Device (IED)
  - …
- The terms SCADA and ICS are often used interchangeably



[Stouffer et al. 2008]

Good Morning with ICS [Luiijf & Paske 2015]

What ICS controlled functions did you use this morning before you arrived at your desk? None? Then, we ask you to re-trace your steps.

Your alarm clock awoke you. You turned on the bedside light. **The required extra Watts were generated, transported and distributed under ICS control**. While you took a shower, **ICS adjusted the drinking water production process and maintained the pressure in the pipelines to your home**. **Heating** of your home and cooking breakfast required the production, transport and distribution of gas. All these processes are controlled by ICS. The cup of milk you used required **automatic milking, strict temperature control of the intermediate storage tanks**, and **processing and packaging at the milk factory**, all under ICS control. You either took the **train (ICS-controlled signalling, points, power and traction)**, or **road transport (ICS-controlled traffic lights, safety systems in tunnels and traffic control of lanes)**. Arriving at the office, you passed the **ICS-operated barrier to the parking lot** and the **ICS-controlled security barrier or doors** to enter the premises. The **air conditioning, fire protection** and **evacuation systems** of your organisation are all operated by ICS 24/7, as well as **the elevator** you took to your office at the top floor. The (critical) **large coffee/tea/chocolate/soup machine** has embedded ICS and is connected to the Internet …

You may have noticed that we deliberately skipped at least twenty other ICS operated functions your organisation and you have encountered and used this morning. Can you name them? Surprised by how ICS embed and hide themselves in functionality that is taken for granted?

But who is taking care of the cyber security and resilience of such critical functions? Or are these ICS managed in an unconsciously insecure way?

Outline

- What is a Critical Infrastructure (CI)?
- CIs and Industrial Control Systems (ICSs)
- **Cyber Security of CIs and ICSs**
    - Stuxnet
    - BlackEnergy

Cyber Security of CIs and ICSs

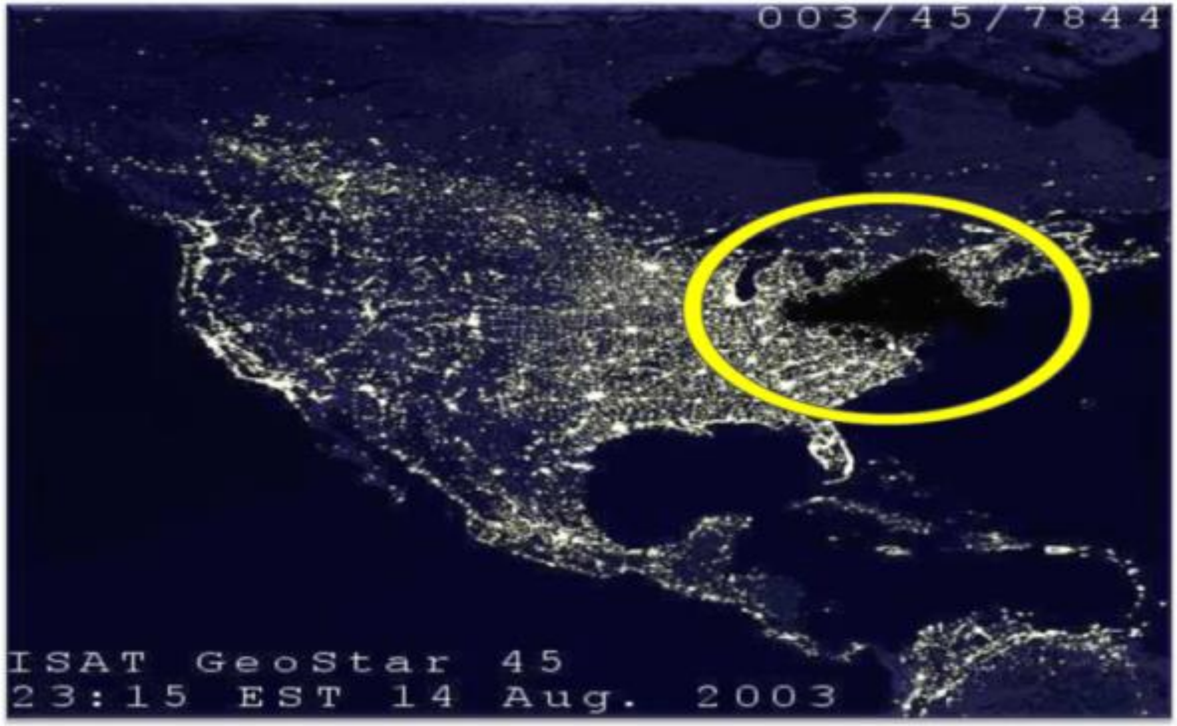
- Security through obscurity
  - They use proprietary and not well known software, interfaces and protocols
  - Hence an attacker should
    - Gather knowledge on system design
    - Access the system and learn how it works

- Not really secure…
  - Vendors publish manuals online
  - IP leak
  - Some devices can be bought cheaply

"systems and software that have not had the trial by fire of exposure to the Internet and outside attackers may very well be weaker for lack of having had their security flaws pointed out to the manufacturer" [Andress & Winterfield 2014]

Cyber Security of CIs and ICSs

- What if a SCADA fails?
- The Northeast Blackout of 2003
  - Failure in a software monitoring system at a utility company in Ohio, outage at a local power plant
  - Power to be drawn from other plants in the area
  - Heavily loaded power lines sag, come into contact with improperly trimmed trees, and fail
  - Utility systems in Ohio begin to draw power from the systems in Michigan, load balancing issues
  - Other lines failed in Ohio and Michigan, causing power generating stations to go offline
  - Power routed from plants on the east coast, causing overloads and plants shut down
  - Grids in Michigan and Ohio disconnected from each other
  - Grids in Canada disconnected as well
  - Grids in Ontario, New York, New England, Windsor, New Jersey, and Philadelphia were affected



homesecurity.press

Extremely complex interdependencies
→ large-scale, unexpected domino effect

Outline

- What is a Critical Infrastructure (CI)?
- CIs and Industrial Control Systems (ICSs)
- Cyber Security of CIs and ICSs
    - ➢ **Stuxnet**
    - ○ BlackEnergy

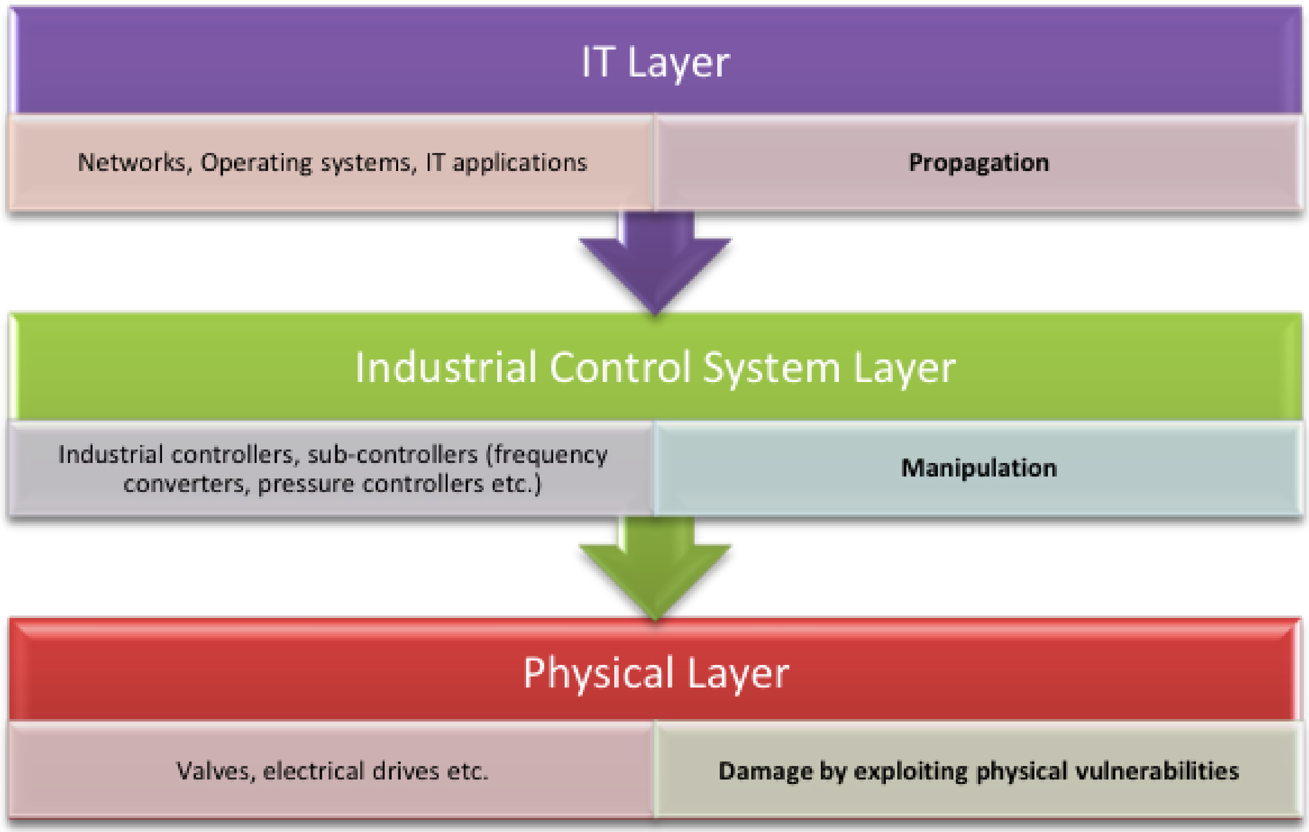
Stuxnet

- Cyber attacks against Iranian nuclear facilities, at Natanz, during 2009 and 2010
- Goal: damage centrifuges used for uranium enrichment, to hinder Iran’s nuclear program
- Attack development cost estimated in millions of USD
- Highly sophisticated malware, several zero-day exploits

www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html

Stuxnet

- The nuclear facility includes an Industrial Control System
  - ICS not connected to the Internet
  - Physical equipment operated by assembly code on PLCs
  - PLCs programmed from Field PGs, not connected to the Internet
- Stuxnet infection
  - Maybe through USB devices
  - Spread over LAN
  - Look for Siemens Step7 software



IT Layer

Networks, Operating systems, IT applications — Propagation

Industrial Control System Layer

Industrial controllers, sub-controllers (frequency converters, pressure controllers etc.) — Manipulation

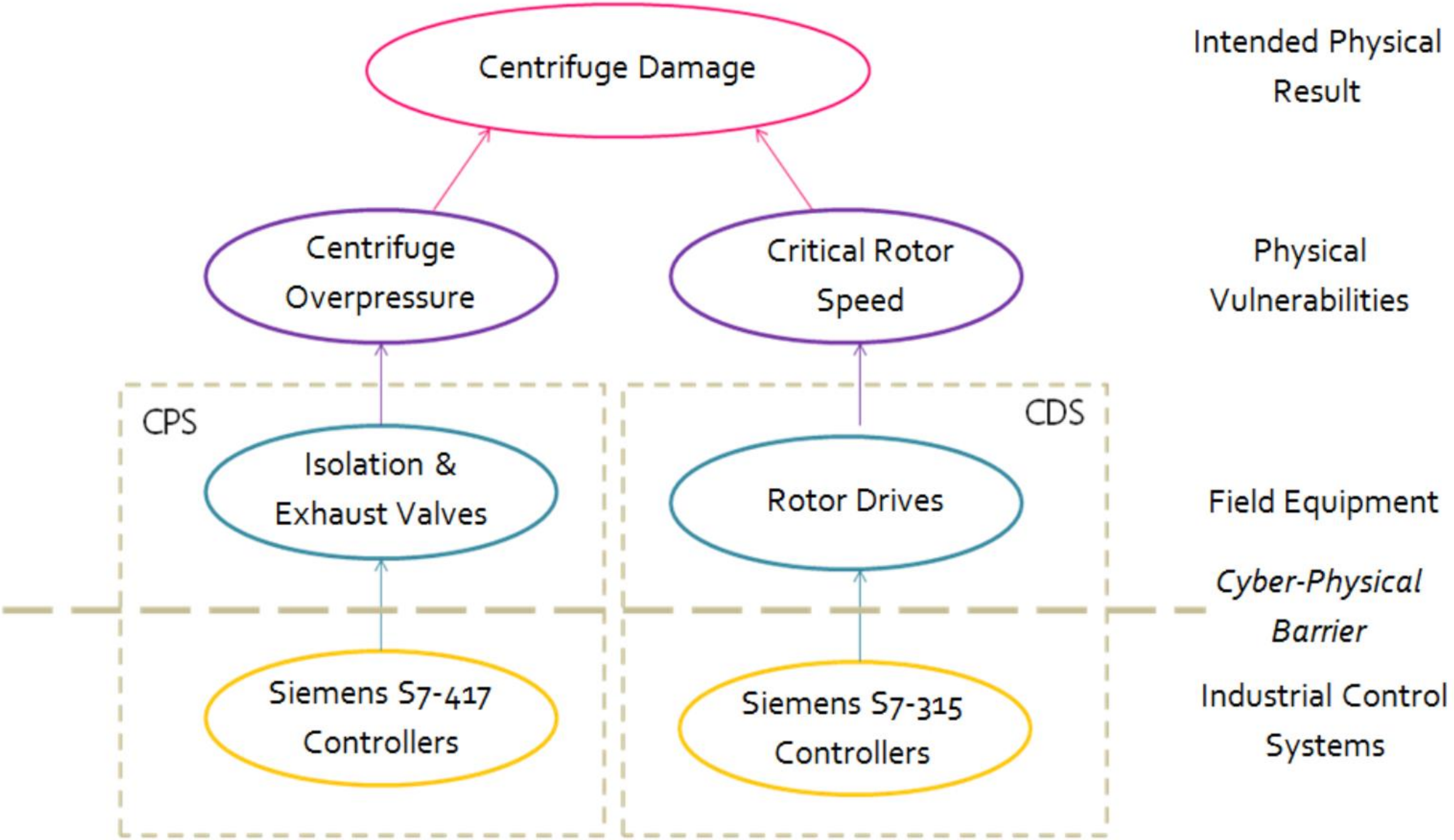
Physical Layer

Valves, electrical drives etc. — Damage by exploiting physical vulnerabilities

igure 1: The three layers of a sophisticated cyber-physical attack

[Langner 2013]

Stuxnet



[Langner 2013]

Stuxnet

- Attacker’s intention was not to destroy the nuclear facility, rather to stealthily and slowly damage the enrichment process

- Stuxnet exemplified a methodology for cyber-physical attack engineering which is likely to work again
    - Physical vulnerabilities of course depend on the specific target
    - No zero-days in ICSs, just legitimate features have been used
    - Indirect infiltration via soft targets, e.g. the weak links in the supply chain

- Do future Stuxnet-scale attacks require a state actor to pull them off?

Stuxnet

- Why a malware? Why not an air strike?
    - Much higher development costs
    - Casualties, injuries
    - Likely loss of employed weapons/equipment
    - Severe retaliation
    - Other collateral damages (e.g. oil price increase)

- Attack's overall effect not impressive
    - Damaged centrifuges replaced and uranium enriching process resumed
    - Lack of really coercive power

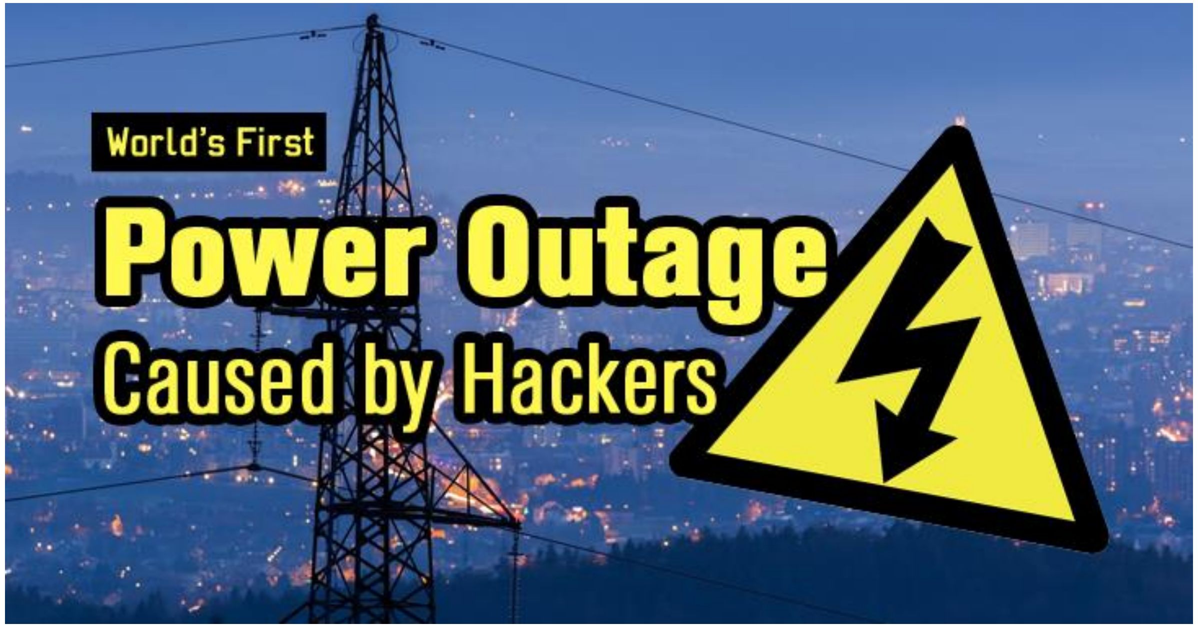
- Cyber weapons can be copied and their proliferation cannot be controlled

Outline

- What is a Critical Infrastructure (CI)?
- CIs and Industrial Control Systems (ICSs)
- Cyber Security of CIs and ICSs
  - Stuxnet
  - **BlackEnergy**

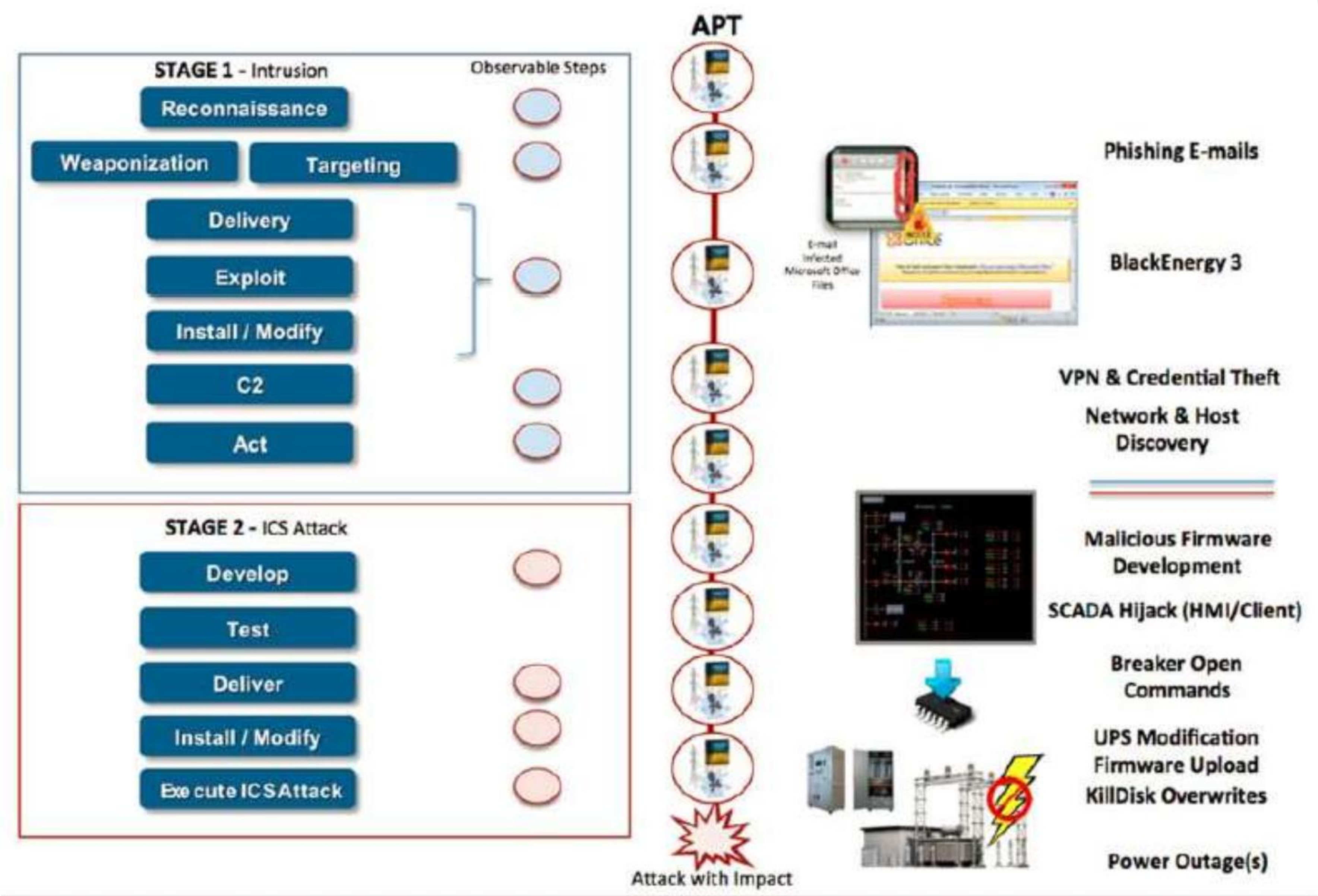
Power Outage in Ivano-Frankivsk Region of Ukraine

- December 23rd, 2015
- Three energy distribution companies attacked
- Approximately 225,000 customers lost power for 1 to 6 hours
- The attack at a glance
    - Energy substations switched off
    - IT infrastructure component disabled
    - Files removed
    - DoS on call-centre



thehackernews.com/2016/01/Ukraine-power-system-hacked.html

BlackEnergy



[Paladion 2015]

BlackEnergy

Lessons Learned

- Need to train end users to recognise phishing attacks
- Use end point protection solutions with anti-malware and application whitelisting to detect/prevent installation of malicious software program
- Use intel to detect anomalies in network traffic e.g. sudden increase in outgoing data size, unusual traffic protocols in use, etc.
- Adequately segregate IT network & SCADA network
- Use 2-factor authentication for VPN connections
- Implement sessions timeouts of VPN connections
- Implement SoD in SCADA applications to limit privileges of a single role
- Avoid allowing use of vendor default or shared userid & password in Operator or Engineering workstations

Security of Critical Infrastructure – Recap

- What is a Critical Infrastructure (CI)?
  - [UK] National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends
- CIs and Industrial Control Systems (ICSs)
  - Many CIs are controlled and monitored by Industrial Control Systems (ICS)
- Cyber Security of CIs and ICSs
  - Stuxnet
  - BlackEnergy

Security of Critical Infrastructure - References

- Centre for the Protection of National Infrastructure (www.cpni.gov.uk)
- E. Luiijf, B. J. Paske, “Cyber Security of Industrial Control Systems”, 2015
- K. Stouffer, J. Falco, K. Kent, K. “Guide to Industrial Control Systems (ICS) Security Recommendations of the National Institute of Standards and Technology”, NIST Special Publication, vol. 800, 2008
- J. Andress, S. Winterfield, “Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners”, 2014
- R. Langner, “To Kill a Centrifuge, A Technical Analysis of What Stuxnet’s Creators Tried to Achieve”, 2013
- Paladion, “Black Energy - Pushing the Country to Total Darkness”, 2015