Cyber Threat Intelligence and Threat Hunting in the Energy Domain

CSP006_S_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Acknowledgement

- *Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Cyber Threat Intelligence and Threat Hunting in the Energy Domain

Overview

- Topic-1: Introduction to Threat Intelligence and Threat Hunting
- Topic-2: Data Sources and Collection
- Topic-3: Threat Actors and Tactics
- Topic-4: Practical Threat Modelling and Security Investigation

Agenda

01. Why should my company be a target of a cyber-attack?

02. Threat Actors

03. Exercise: Cyber Kill Chain

Why should my company be a target of a cyber-attack?

Why?

Why should my company be a target of a cyber-attack?

… because your data is valuable

- Customer databases, profiles, credit card data
- Strategic plans, financial situation
- Research & development data

… because your company‘s loss is another‘s gain

- Competitors, market value
- Political/terrorist organizations

… because you have IT ressources that can be reused to

- distribute illegal content
- attack thrid party systems creating the impression it was you
- sell your internet connection bandwidth for botnet usage (DDoS, cryptominer, etc.)

… because it‘s easy and automatable

- e.g. ransomware, spam-lists, …

The need for **controls**

Road safety

Technical controls

- Active safety controls
  - ABS, ASR, ESP, etc.
- Passive safety controls
  - Airbag, seatbelt, booster seat, rearview mirror, etc.

INFORMATION SECURITY

Technical controls

Active safety controls

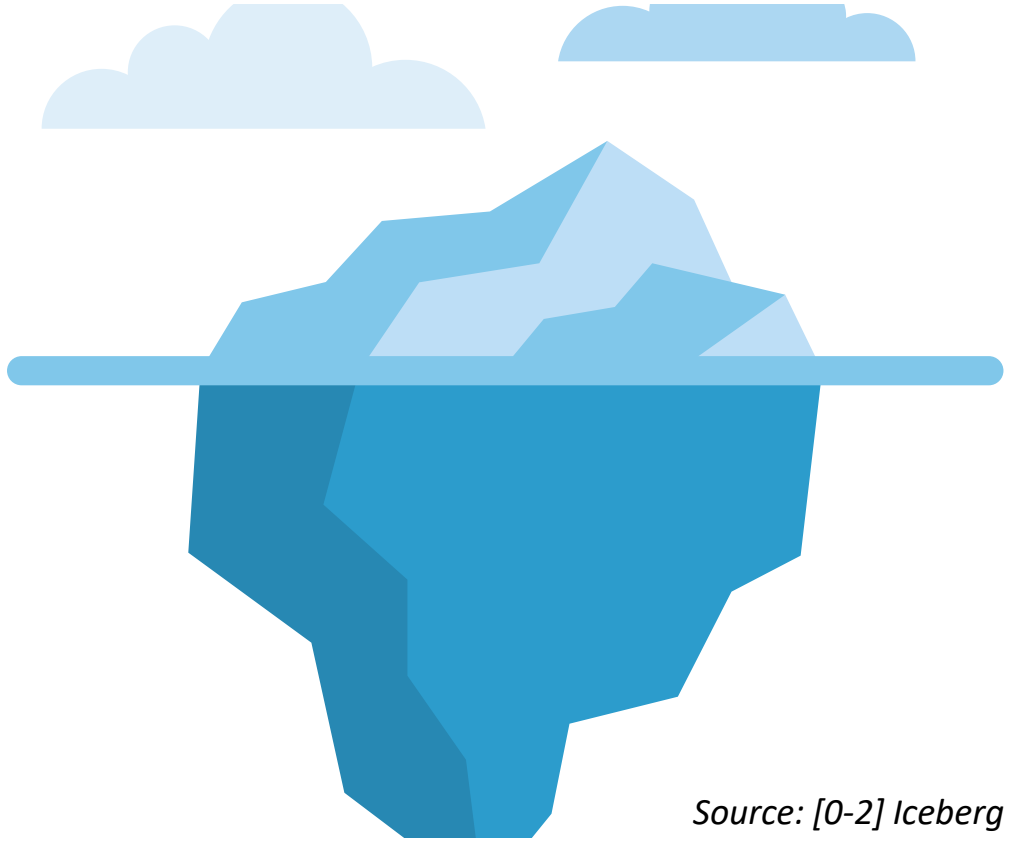
Access control systems, firewalls, antivirus, spam protection, IPS, etc.

Passive safety controls

Identity management systems, security audits, log files, redundancy, IDS, etc.

Accessibility of Information

- **Clear** Web
  - Indexed by search engines
- **Deep** Web
  - Not indexed by search engines
- **Dark** Web/Net
  - TOR network .onion address
  - Invitation / vetting process

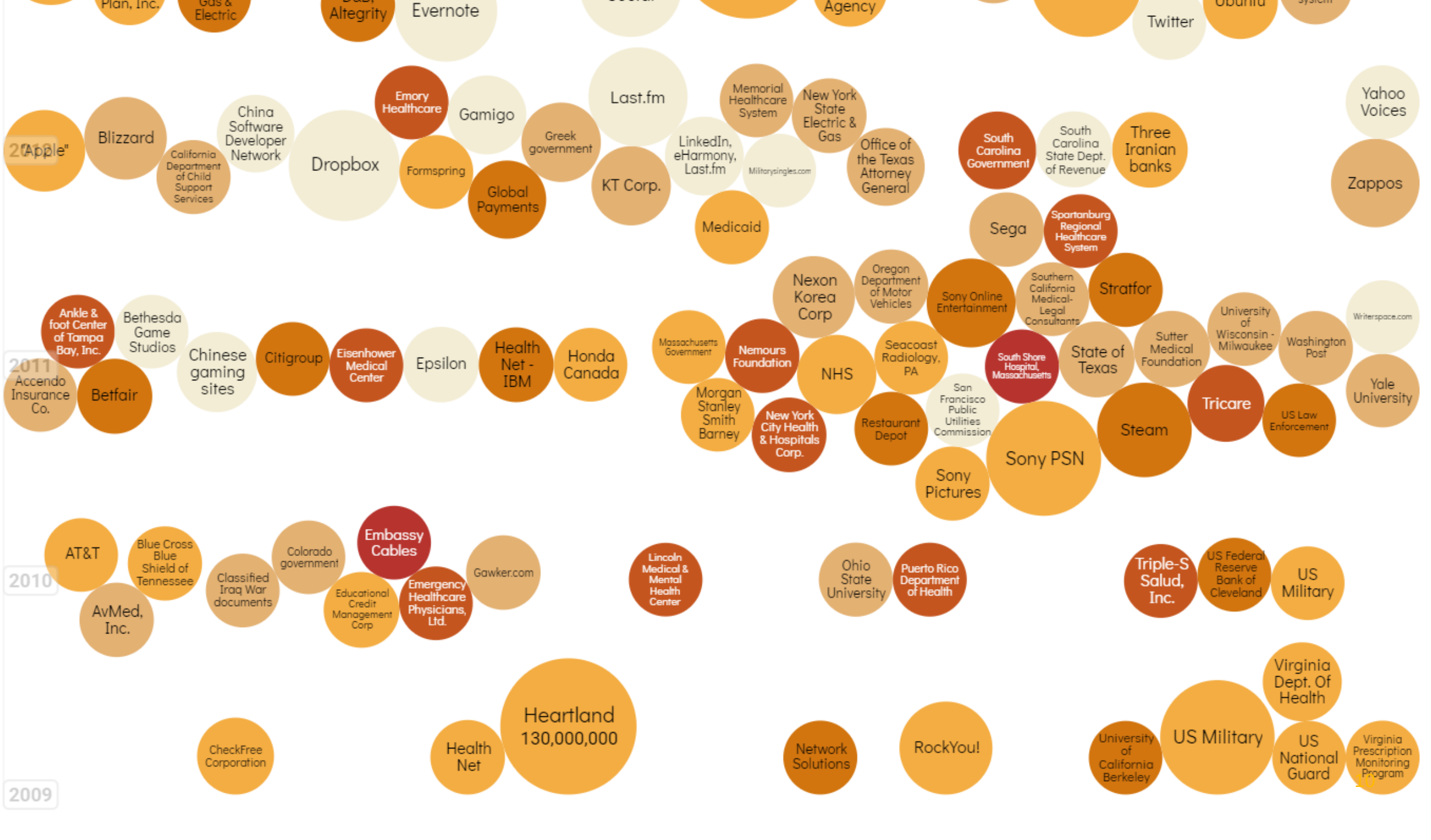


Source: [0-2] Iceberg

Current Cyber Security **Landscape**

- Perimeter protection centralized view is obsolete
  - Endpoint detection & response
- Data losses, intrusions and privacy violations go through the roof
  - Most intrusions are not detected in a timely manner
  - Just a few examples of those we know of…

Next Slide Source:
[1] InformationIsBeautiful.net


Plan, Inc.
Gas & Electric
Altegrity
Evernote
Agency
Twitter
Ubuntu
2012
"Apple"
Blizzard
California Department of Child Support Services
China Software Developer Network
Dropbox
Emory Healthcare
Formspring
Gamigo
Global Payments
Greek government
Last.fm
KT Corp.
LinkedIn, eHarmony, Last.fm
Medicaid
Memorial Healthcare System
Militarysingles.com
New York State Electric & Gas
Office of the Texas Attorney General
South Carolina Government
South Carolina State Dept. of Revenue
Three Iranian banks
Yahoo Voices
Zappos
Sega
Spartanburg Regional Healthcare System
Nexon Korea Corp
Oregon Department of Motor Vehicles
Sony Online Entertainment
Southern California Medical-Legal Consultants
Stratfor
Writerspace.com
University of Wisconsin - Milwaukee
Washington Post
Yale University
Sutter Medical Foundation
State of Texas
South Shore Hospital, Massachusetts
Tricare
US Law Enforcement
Steam
Sony PSN
Sony Pictures
San Francisco Public Utilities Commission
Restaurant Depot
Massachusetts Government
Nemours Foundation
NHS
Seacoast Radiology, PA
Morgan Stanley Smith Barney
New York City Health & Hospitals Corp.
2011
Ankle & foot Center of Tampa Bay, Inc.
Bethesda Game Studios
Accendo Insurance Co.
Betfair
Chinese gaming sites
Citigroup
Eisenhower Medical Center
Epsilon
Health Net - IBM
Honda Canada
2010
AT&T
Blue Cross Blue Shield of Tennessee
AvMed, Inc.
Classified Iraq War documents
Colorado government
Embassy Cables
Educational Credit Management Corp
Emergency Healthcare Physicians, Ltd.
Gawker.com
Lincoln Medical & Mental Health Center
Ohio State University
Puerto Rico Department of Health
Triple-S Salud, Inc.
US Federal Reserve Bank of Cleveland
US Military
2009
CheckFree Corporation
Health Net
Heartland 130,000,000
Network Solutions
RockYou!
University of California Berkeley
US Military
Virginia Dept. Of Health
US National Guard
Virginia Prescription Monitoring Program

Threat Actors

Threat **actors, attribution & obfuscation**

Threat actors:	**Motivation:**
Nation-States	Geopolitical
Cybercriminals	Profit
Hacktivists	Ideological
Terrorist Groups	Ideological, including violence
Thrill-Seekers	Satisfaction
Insider Threats	Discontent
Script Kiddies	Egotism

Nation State Threat Actors

Most capable threat actor due to available resources

Depending on organizational context - worst case estimation regarding threat capabilities and motivation

Currently, countries with the most resources, offensive capabilities and active engagements

- United States of America
- Russia
- China
- North Korea

Nation-state cybersecurity threat actors 2019 – **United States**

United States of America

- As shown during the last years by Edward Snowden and various other leaks on US cyber threat capabilities, the resources and capabilities of the US are enormous
- This was recently shown by the U.S. cyber-attack on foreign infrastructure that followed the attacks on US oil tankers

Nation-state cybersecurity threat actors 2019 – **Russia**

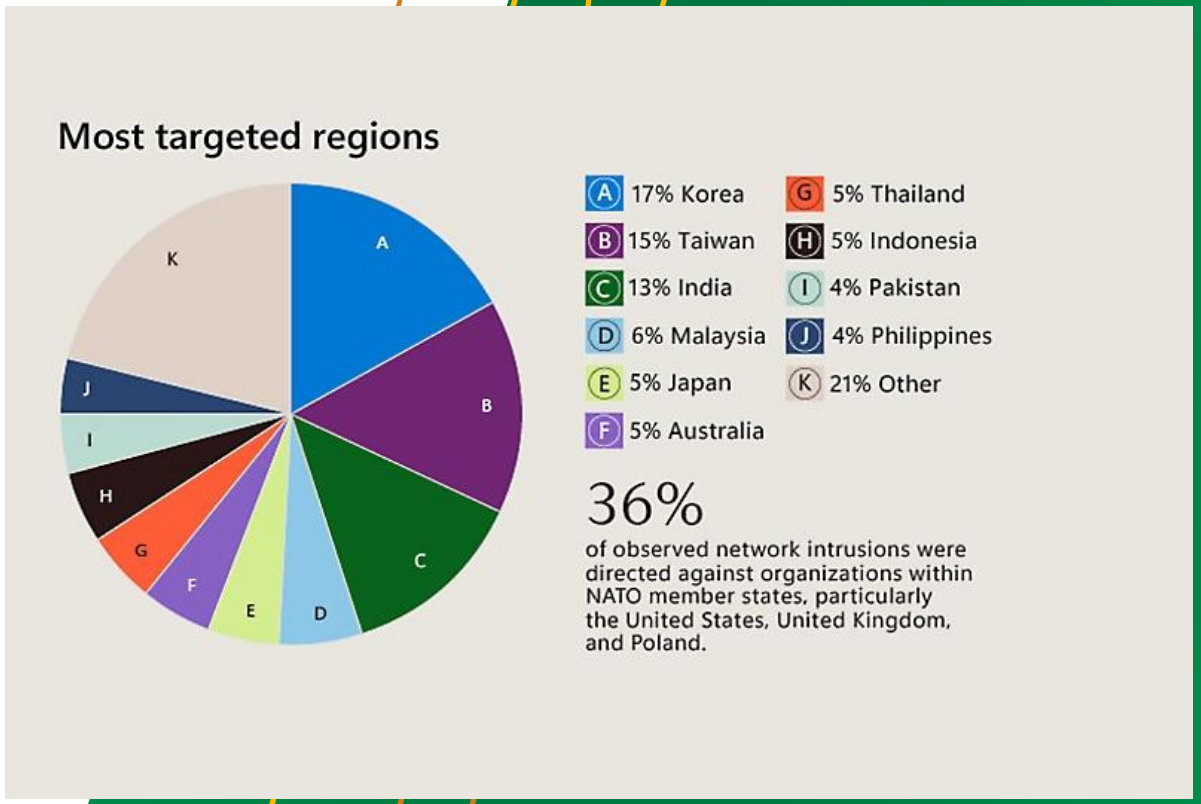
Russia

- Russia uses cyberspace as one of many methods for obtaining the necessary know-how and technology to grow and modernize its economy, especially in
  - defense industry,
  - energy,
  - healthcare, and
  - technology sectors
- Other prominent examples include the caber attack on the Ukrainian water grid as well as electronic warfare tests in Syria

Nation-state cybersecurity threat actors 2023 – **Russia**

Russia

- Russian state-sponsored threat actors employed various tactics, including phishing campaigns and zero-day exploits.
- Their objective was to gain initial access to devices and networks in industries within NATO member states.
- Additionally, malign influence actors targeted the Ukrainian diaspora to intimidate them and incite protest movements across Europe.



Nation-state cybersecurity threat actors 2019 – **China**

China

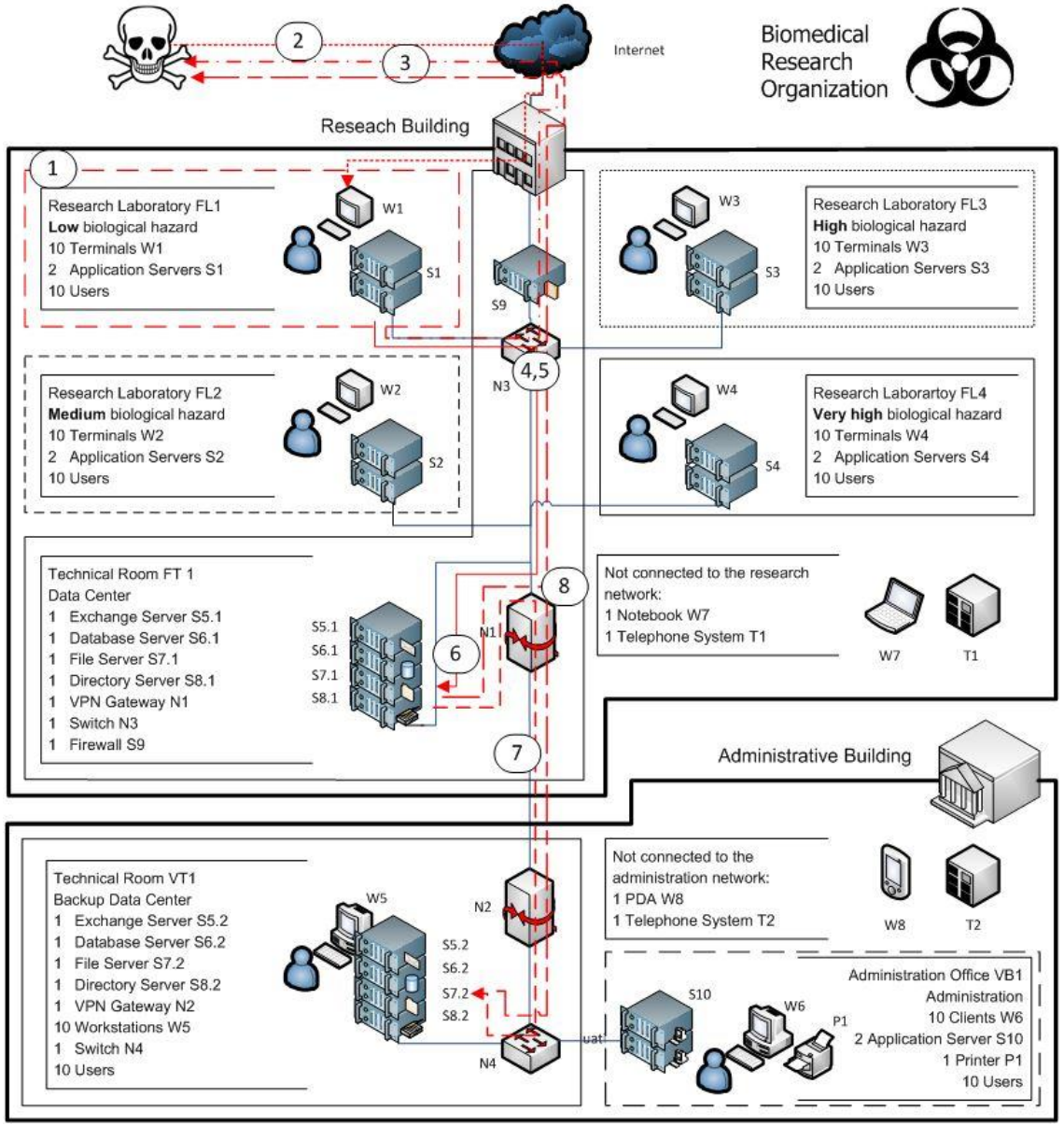
- China continues to use cyber espionage to support its strategic development goals
  - science and technology advancement,
  - military modernization, and
  - economic policy objectives
- Cybersecurity researchers have also recently found links between Chinese cyber actors and a back door a popular application (CCleaner) that allowed the actors to target companies including Google, Microsoft, Intel and Vmware
- APT1

Nation-state cybersecurity threat actors 2019 – **North Korea**

North Korea

- Cyberattack on the South Korea Hydro and Nuclear Power plant in December 2014
- In late 2016, North Korean hackers managed to gain access to a *secure* South Korean military computer network
  - extracted data included contingency plans for a strike against the North's leaders in the event of a border war
- During 2019, a large number of attacks on cryptocurrencies as well as ransomware infections were attributed to North Korean state-sponsored hackers

Typical Attack **lifecycle**



1: **Initial Recon** – get information about the target
2: **Initial Compromise** – spear phishing mail to user, client exploit connects to adversary's C&C server
3: **Establish Foothold –** adaption to system, standard backdoor installation
4: **Escalate Privileges** – user names, password combinations gathered
5: **Internal Recon** – authentication and network structure gathered
6: **Move Laterally** – adversary infiltrates local and backup data center
7: **Maintain Presence** – all tracks are covered up, adversary silently stays in.
8: **Complete Mission** – all target information is collected, export via covert channels, traces will be erased

Cyber threat **buzzwords**

- Adware & ultrasonic cross device recognition
- Backdoors
- Bots and Botnets
- Code injection
- Crypto mining
- (D)DoS & amplification attacks
- Drive-by exploits / watering hole
- Exploits & obfuscation kits
- Man-in-the-Middle
- Password cracking
- Pharming
- Phishing, Spoofing, Spear-Phishing, Whaling, Smishing
- Ransomware
- Rootkit
- Spyware
- SSL hijacking
- Typo-sqatting
- Malware - Virus, worm, payload, trojan
- WiFi eavesdropping & hacking
- Zero Days

Other important R&D

Deep fakes
- picture/video/voice
  - https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

Light commands
- https://lightcommands.com/

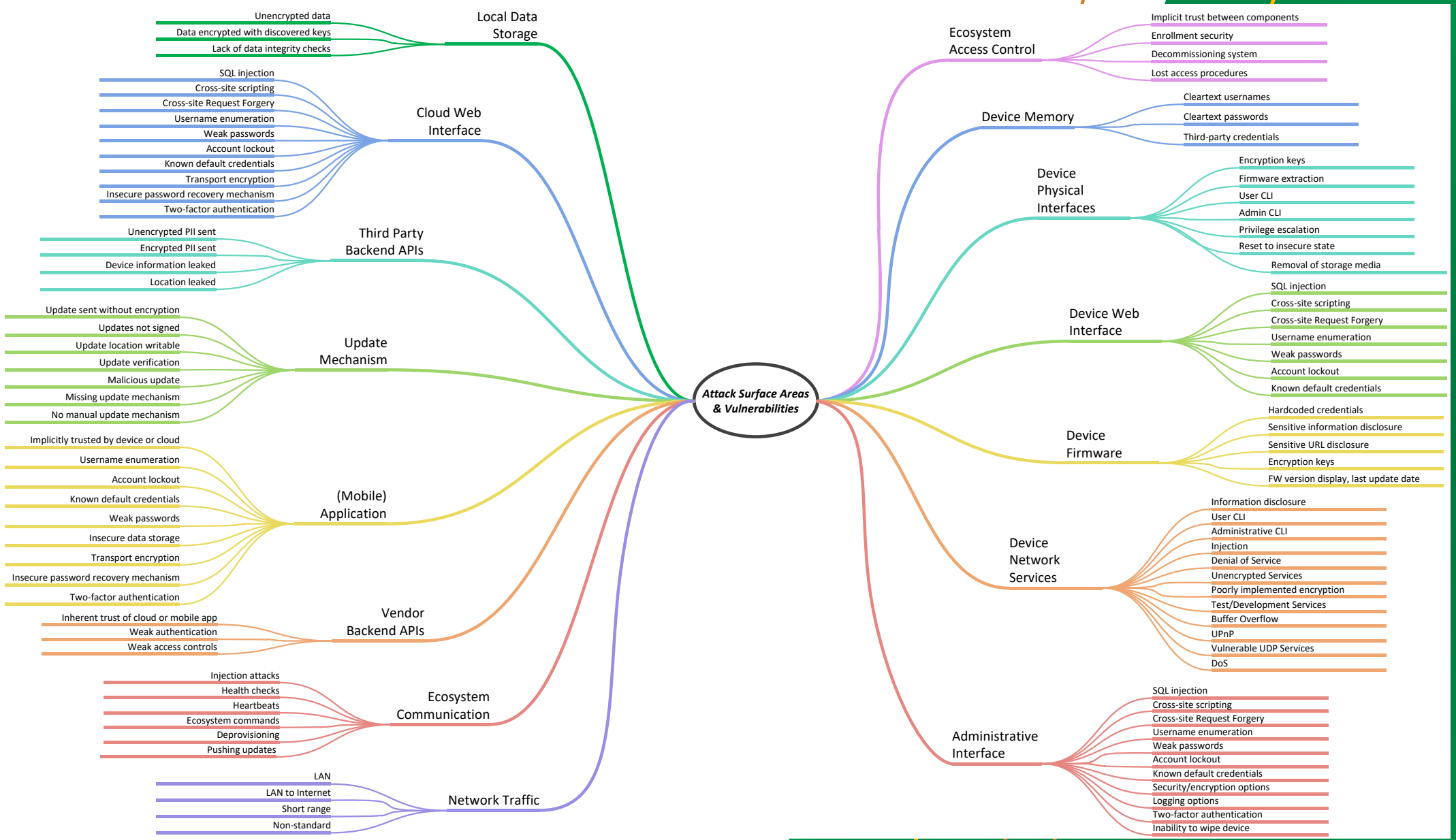
Weaponization of AI
- Autonomous drone capabilities
- Berkley University - Slaughterbots
  - https://www.youtube.com/watch?v=HipTO_7mUOw

DARPA Electronics Resurgence Initiative
- https://www.darpa.mil/work-with-us/electronics-resurgence-initiative

China's foreign tech policy
- https://www.cnbc.com/2019/12/09/china-reportedly-orders-state-offices-to-remove-foreign-tech.html

Banking MFA app requirement due to SIM-Swapping incidents
- EU Payment Services Directive

First official act of cyber war (US -> IRAN)
- https://www.bbc.com/news/world-us-canada-48735097



The MITRE **ATT&CK Matrix** for Enterprise

MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search site

MATRICES

- PRE-ATT&CK
- Enterprise
  - All Platforms
  - Windows
  - macOS
  - Linux
  - Cloud
- Mobile

Home > Matrices > Enterprise

Launch the ATT&CK™ Navigator

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe

Source: [2] attack.mitre.org

Exercise: Cyber Kill Chain

Exercise: Cyber **Kill Chain**

- Everyone model a fictitious attack scenario (cyber kill chain) based on the attack lifecycle stages of the MITRE Att&ck matrix
  - read about / pick your favorite tactics and
  - come up with a short PowerPoint presentation of a (plausible) attack scenario - describe
    - a fictitious company and what they do
    - the type of information under attack / attacker motivation,
    - how they covered all or most of the lifecycle stages (initial access, execution, etc.)

Intrusion patterns – in general

Further, detailed knowledge base on attack methods, tactics, techniques and defenses

- Tactics
  - https://attack.mitre.org/tactics
- Attack matrix
  - https://attack.mitre.org/matrices
- Mitigation strategies
  - https://attack.mitre.org/mitigations

Connect with CyberSecPro:
How to register and other practical information

1. Website:
   www.cybersecpro-project.eu
2. X (Twitter):
   https://twitter.com/CyberSecPro_eu
3. LinkedIn:
   https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

Please send all questions to:
Stefan Schauer
Stefan.Schauer@ait.ac.at
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at