Cyber Warfare

Finse Cybersecurity Winter School 2022

Audun Jøsang
University of Oslo

Information Warfare

- NATO term: Information Operations

- US term: Information Warfare

Information Warfare

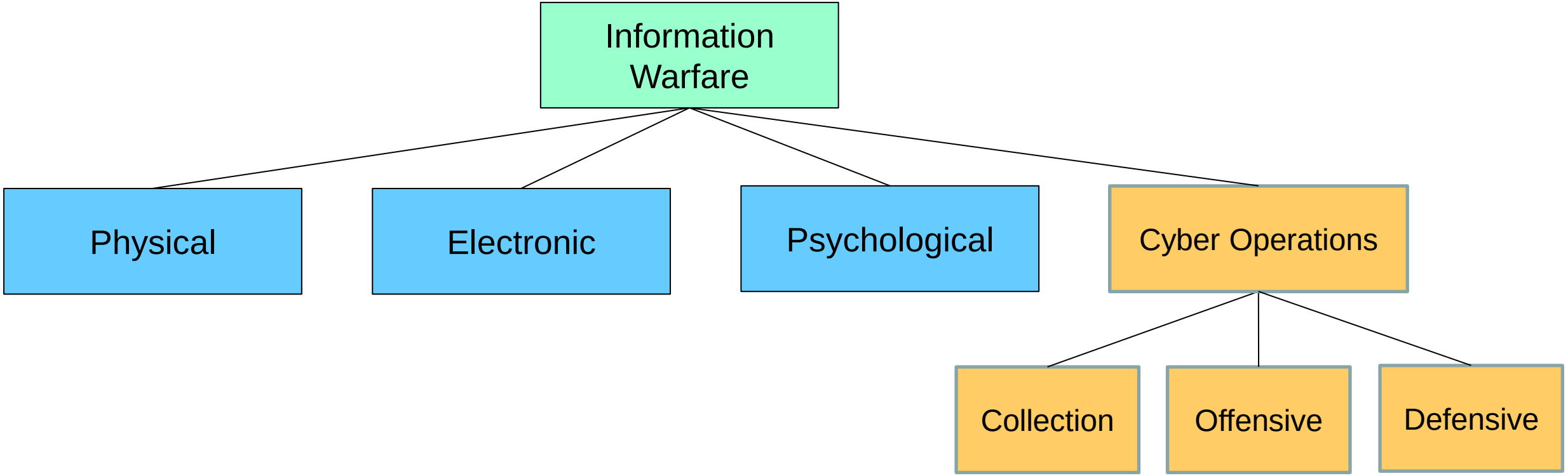
- Physical, e.g. bombing communications infrastructure,
- Electronic, e.g. jamming (disturbance) of radio communications
- Psychological operations (PsyOps), e.g. propaganda
- Cyber Operations = Computer Network Operations

Cyber Operations
aka. Computer Network Operations (CNO)

- Computer Network Operations
  (NATO Allied Joint Publication)
  - Computer Network Espionage (CNE)
  - Computer Network Attack (CNA)
  - Computer Network Defense (CND)

- Cyber Operations
  (US Cyber Operations Policy)
  - Cyber Collection
  - Offensive Cyber Effects Operations (OCEO)
  - Defensive Cyber Effects Operations (DCEO)

Concepts Overview



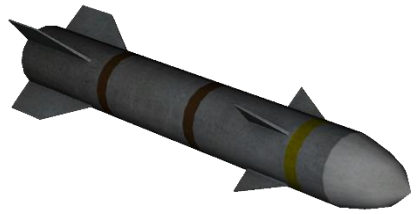
Attribution of Cyber Operations

- The Fog of Cyber Warfare
  - Abstract distance between threat actors (decision makers and executors) and victims/targets of cyber operations
  - Victims are faced with plethora of competing hypotheses about identity and intent of threat actors.
  - Wrong attribution of attacks can cause unintended damage

- Cyber attack reverse-engineering
  - Attribution and understanding the intent of attack
  - Based on analysis if observed indicators, and CTI (Cyber Threat Intelligence)
  - Challenging because
    - Attacks can be channelled through multiple channels and nodes to confuse back-tracking
    - Deliberate misrepresentation of attack indicators

Nature of Cyber Weapons

- Effect of cyber vs. traditional weapons
  - Ballistic missiles cause direct physical damage (material)
  - Cyber weapons only cause direct breach of CIA (immaterial)
    (CIA = Confidentiality, Integrity, Availability of information)
  - Ballistic missiles are destroyed in the attack
  - Cyber weapons can be reused/recycled and used to attack others



- Weapons can be either hidden or observable
  - Observable weapons give deterrence, but can be attacked
  - Hidden weapons can give effect of surprise, but little deterrence
  - Cyber weapons are typically hidden. Deterrence requires openness

- Steady supply of weapons needed
  - Each cyber weapon has a use-by date
  - Cyber weapons typically depend on zero-day vulnerabilities
  - Cyber weapons require steady supply of zero-days → fuzzing

Value of espionage and offensive cyber operations

Cyber Espionage

- Offers huge advantage for intelligence gathering
- Cheaper and less risky than traditional physical espionage

Cyber Sabotage

- Disruption of digital systems and processes
- Attacks on critical infrastructure can be especially damaging
- Impact can be reduced by good preparedness and incident handling
- Considerable resources required by attackers to achieve substantial impact
- Often cheaper to obtain similar impact with physical attacks
- Has the advantage of frustrating attribution

Cyber operations to supporting physical attacks

- Observed use of cyber ops. in current conflicts (Ukraine)
- Considered to be a potent companion to traditional military ops.
- Confuses and disrupts when communication and coordination is most critical

Countries with Cyber Operations Strategies

- Military defense strategies in the 21st century typically includes a cyber operations strategy.
- Only USA seems to have an official Cyber-Operations Policy
- Other countries might think that since cyber operations are invisible, they see an advantage in not publishing their cyber operations strategy.

The New York Times

By DAVID E. SANGER APRIL 24, 2016

ISIS Targeted by Cyberattacks in a New U.S. Line of Combat

The National Security Agency headquarters in Fort Meade, Md. The agency has for years listened to Islamic State militants, but its military counterpart, Cyber Command, will now direct operations against the militant group.

Perception of Cyber Surveillance

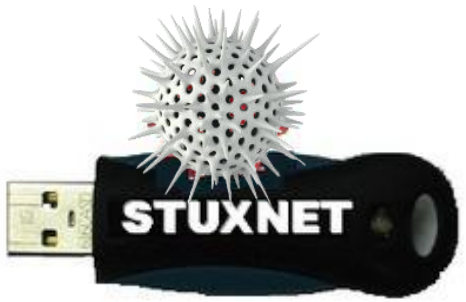
What we thought

What Snowden revealed

Perception of Cyber Attack

What we believe

What if ?



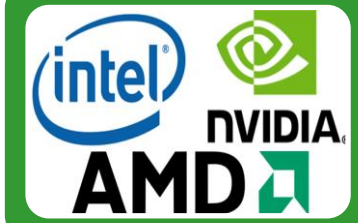
SIEMENS

Microsoft

Potential Cyber Operations Collaboration

OS Vendors

- Software updates, and regular patching
- Potential total control of all online computers



CPU and Microchip Vendors

- Special triggers can open backdoors
- Remote control of computing platforms

Computer System Vendors

- Cyber Ops HW / SW during prod. or shipmnt
- Surveillance or control of computers

Cloud Providers

- Passive or active access to IaaS, PaaS & SaaS
- Surveillance and sabotage in the cloud

Challenge of Industry Collaboration

- Covert cyber operations collaboration
  - Like having a secret affair,
    It's OK as long as nobody finds out
  - Possible reward by government:
    → money and favours

- In case of disclosed cyber operations collaboration
  - Causes embarrassment
  - Loss of trust from market
  - Loss of market share
  - Loss of revenue and profit
  - Legal basis for claiming compensation from government
  - Balkanisation of technology

IT industry politics = national security politics

- Which fighter jet should we buy?

- Which 5G network should we buy?

- Nobel Peace Prize to Liu Xiaobo in 2010 led to 7 years stop in salmon exports to China

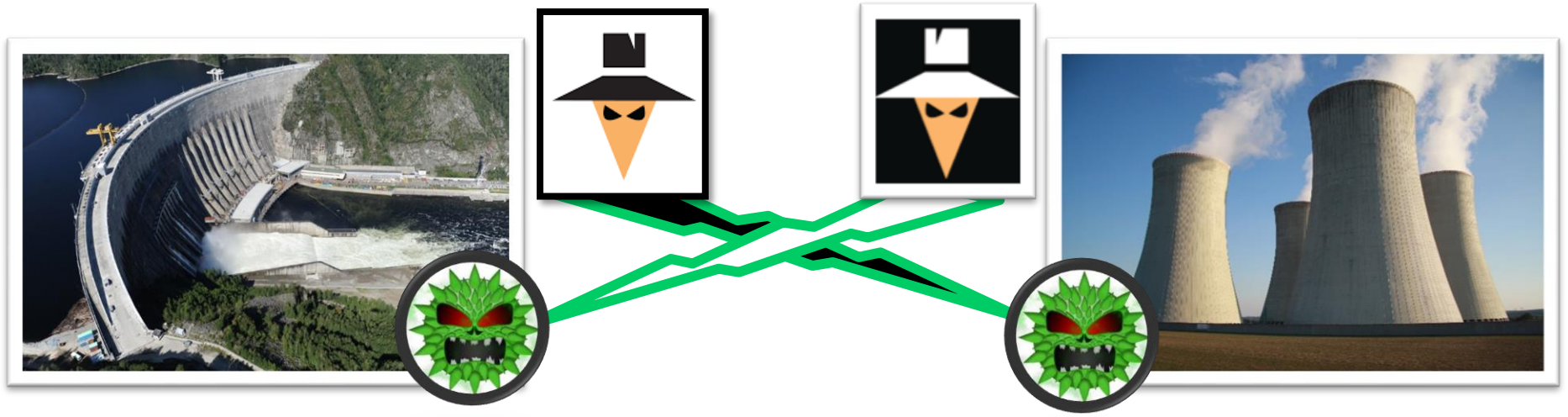
- Boycott of Huawei in 5G and 6G networks can make China implementing more economic and political punishment

Deterrence:

Threat of mutual destruction

- Exchange of signals about credible ability and intent to retaliate
- Assumes that the parties:
  - know each other's assessments and priorities,
  - know each other's capacities and political will to destroy the opponent
  - actually fear destruction
- Terror balance based on deterrence aims to prevent war by making it meaningless to wage war.
- Has prevented the use of nuclear weapons after World War II

Cyber Deterrence



- Russia has been compromising power grids in Western countries since 2014
  - Reports of compromise and espionage against power grids in the United States
  - Sabotage against Ukraine in December 2015
- The United States has been compromising power grids in Russia since 2018
- How do we know that? New York Times article:
  https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html
  - Why? Deterrence!

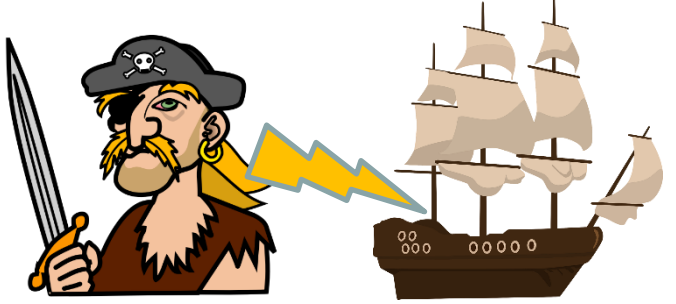
The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections. Maxim Shemetov/Reuters

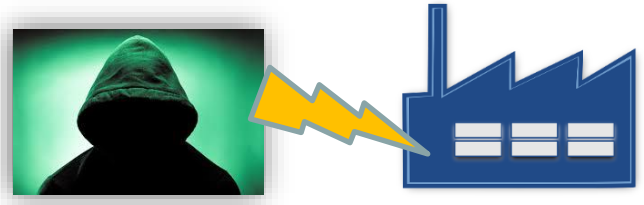
June 15 2019

Cyber Privateering



Privateering 1600 - 1850

- Privateering in the period 1600 - 1800 was piracy committed by private groups with permission from the country's authorities, and was used as a tool in warfare at sea.
- Russian President Putin has stated that Russian groups that carry out cyber attacks on other countries are not considered criminals, "because they do not break Russian law."
- State-sponsored cybercrime can be called *cyber privateering*
- Such cyber operations do not burden the Russian state budget.
- Western countries do not tolerate private groups carrying out cybercrime against other states, regardless of country.
- The Paris Call for Trust and Security in Cyberspace failed because USA/Russia/China want to run cyber operations, and because compliance with a treaty would be difficult to enforce.



Cyber privateering 2020→

Cyber warfare against Ukraine

- In February 2014 the Russian-friendly Ukrainian president Viktor Yanukovych was ousted after the Maidan Revolution because he refused to sign a treaty with the European Union.
- In March 2014, Russia annexed the Crimea peninsula.
- Petro Poroshenko was elected new president in May 2014.
- In 2015 and 2016, a Russian APT (Advanced Persistent Threat) hacked and shut off power to large parts of Ukraine.
- Volodymyr Zelenskyy was elected new president in May 2019.
- On Tuesday 15 February 2022 Russia launched massive cyber attacks against the Defense Ministry, army and national banks.
- On Thursday 24 February 2022 the Russian invasion started.

Yanukovych and Putin

Petro Poroshenko

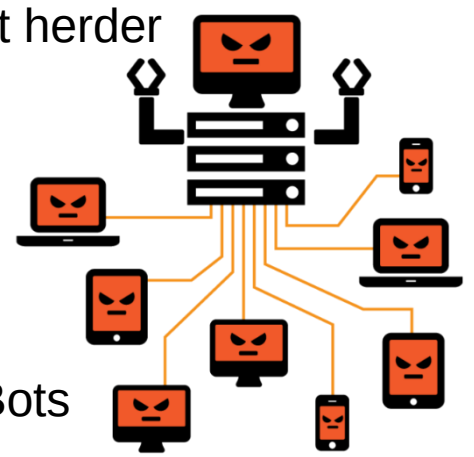
Power grid attacks

Volodymyr Zelenskyy

BigTech takes action

- On Wednesday 23 February, a few hours before Russian tanks began rolling into Ukraine, Microsoft's Threat Intelligence Center found indicators of a never-before-seen piece of "wiper" malware that appeared aimed at the Ukraine's government ministries and financial institutions.
- The Microsoft Threat Intelligence Center quickly picked apart the malware, named it "FoxBlade" and notified Ukraine's top cyberdefense authority.
- The FoxBlade malware was programmed to erase — "wipe" — all data on computers in a network.
- Within three hours, Microsoft's virus detection systems on Windows servers had been updated to block FoxBlade.

FBI disrupts Russian Botnet



- A botnet is thousands of computers with malware which enables the threat actor to control all the computers in a coordinated way
- Botnets are typically used for DDoS attacks (Distributed Denial of Service), where all the infected computers send a flood of traffic to a victim server so that it crashes.
- Russia infected computers all over the world with a bot malware called *Cyclops Blink* to create a huge botnet for DDoS attacks.
- Systems globally, also in Norway, infected with *Cyclops Blink*
- In early April 2022, FBI was able to remove the botnet malware from infected computers, without the owners' knowledge.
- It is normally illegal for FBI to make changes to computers without the owners' knowledge.
- It is plausible that Microsoft helped remove the bot-malware.

Outlook

- Impact of the Russian cyber operations have been relatively limited.
- Did Russia base the success of the invasion on the cyber operations?
- BigTech has played a crucial role for helping Ukraine
- Collaboration with BigTech companies allows highly potent cyber operation
- What will be the role of BigTech in future conflicts between states?