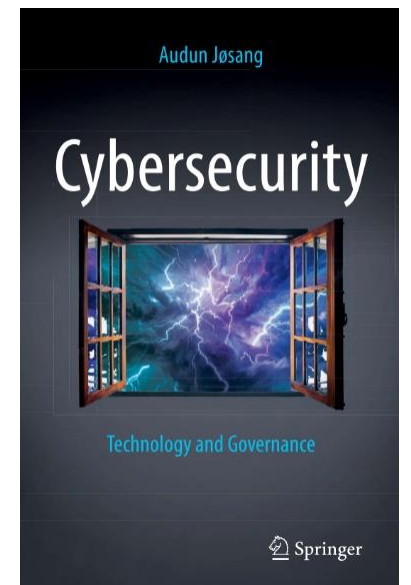


Chapter 16: Cyber Operations

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview

In this lecture, you will learn about

- Cyber operations
- The Cyber Kill Chain
- Advanced Persistent Threat (APT)
- MITRE ATT&CK framework
- Cyber Threat Intelligence
- Cyber Warfare



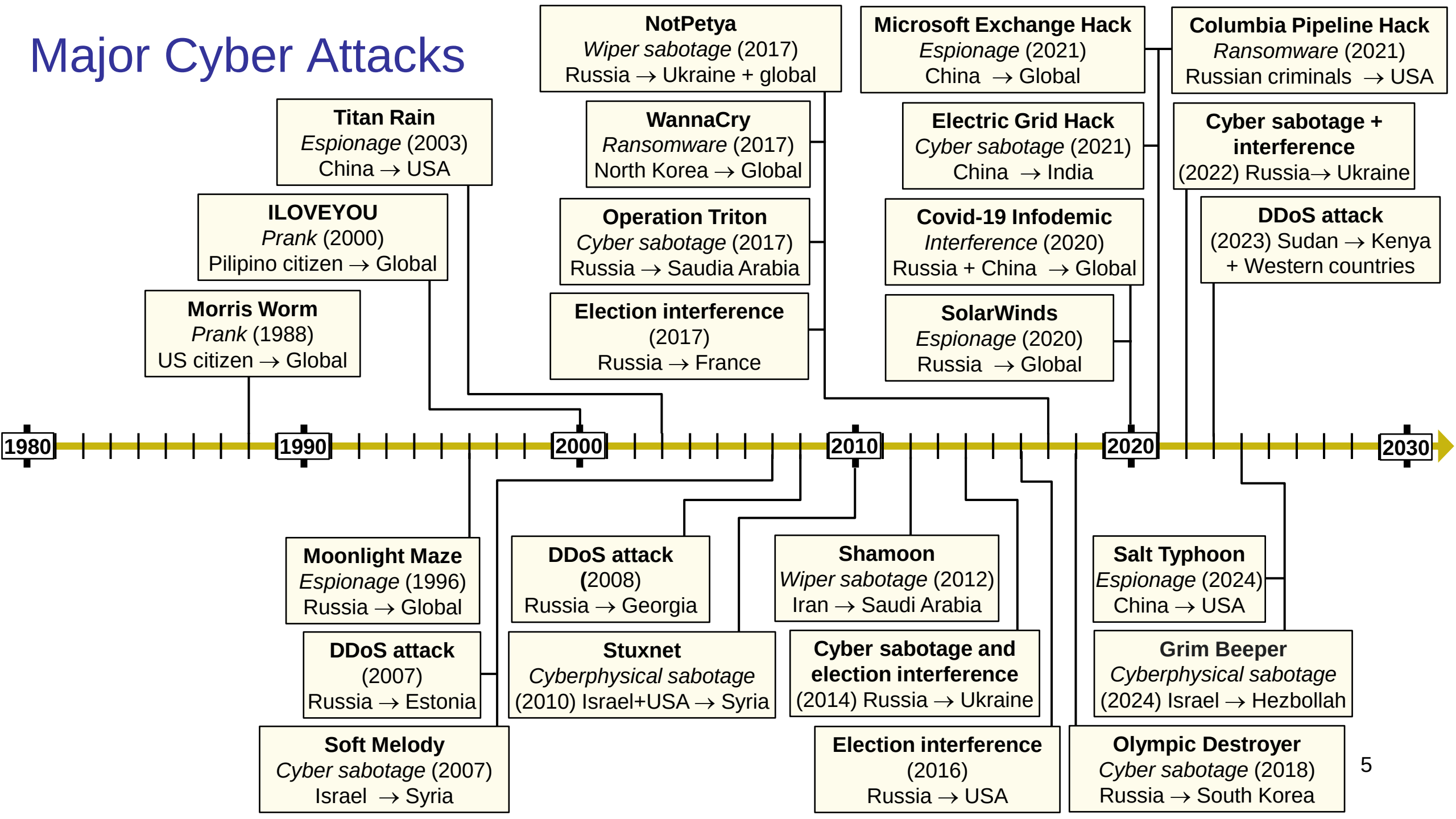
What is a cyber operation?

- "*Cyber operations*" is a rather vague term that is often used for attacks against, and defense of, digital infrastructures.
- Called *offensive* and *defensive* cyber operations in a military context.
- Called *red teaming* and *blue teaming* in the context of training and simulations.
- Offensive cyber operations mean cyber attacks and unauthorised access to information and ICT systems. For example, criminals who carry out cyber attacks for profit or state actors who carry out cyber sabotage.
- Defensive cyber operations mean activities and operations to deal with these data breaches, whether someone is affected, or there is a suspicion that targeted data breaches will happen.

Advanced Attacks / Advanced Cyber Operations

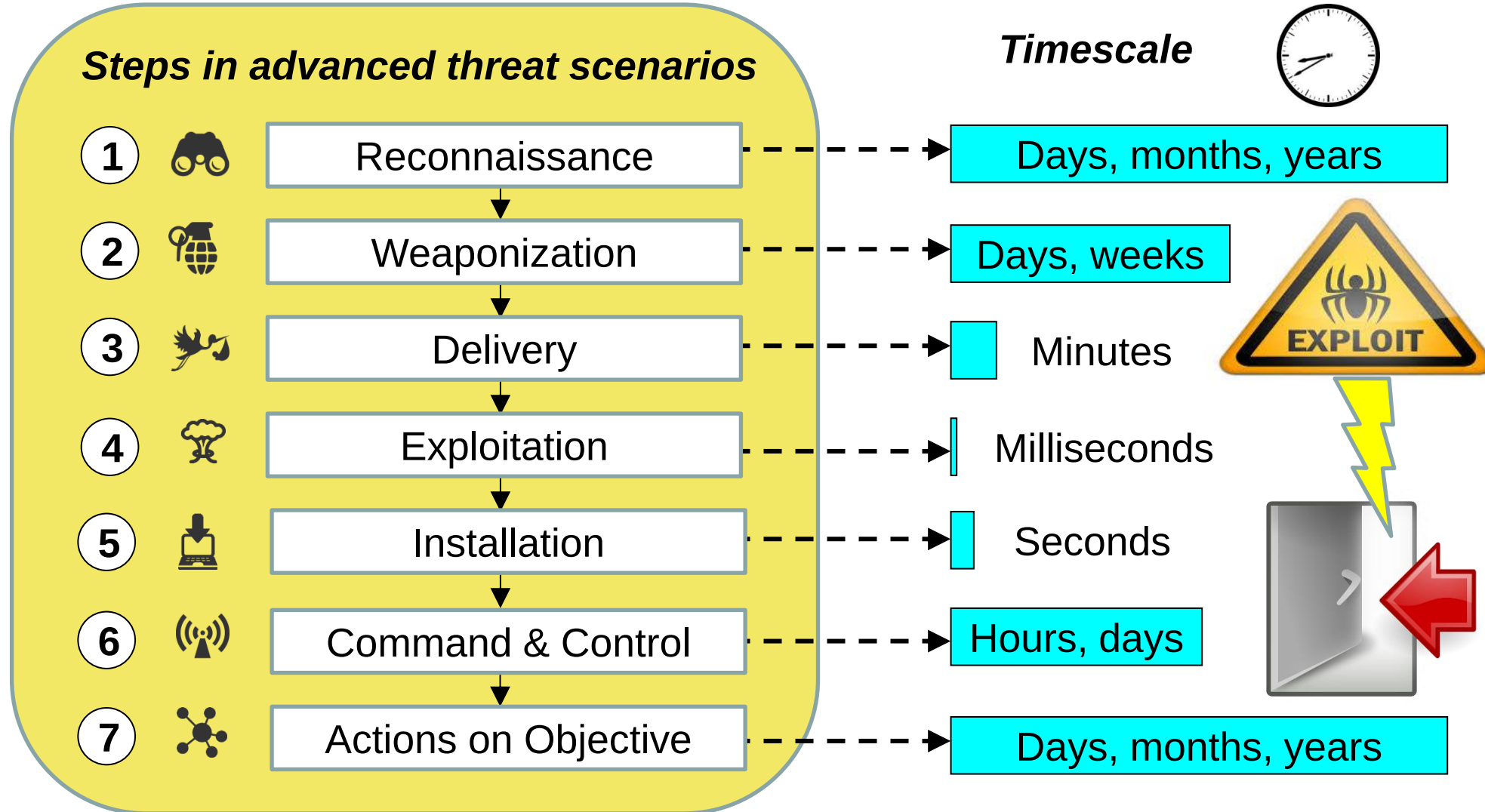
- Adversarial cyber operations are carried out by state (sponsored) actors for espionage, sabotage or financial gain
- They can have disastrous consequences, and can cause collateral damage for victims other than the intended target
- These operations often last for a long time
- ... and is carried out over several steps

Major Cyber Attacks



Cyber Kill Chain

- The Cyber Kill Chain is a model developed by Lockheed Martin.
- The model describes the steps of an advanced targeted cyber attack.
- The attack can be interrupted at each of these steps
 - The earlier the better



<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

CKC Step 1. Reconnaissance

- The threat actor selects the potential victim
- Collects information and "researches" it
- Attempts to identify vulnerabilities in the network that can be exploited
- May involve scanning infrastructure, using news, social media, etc.
- Example:
 - A company is chosen as target for getting specific information for use in crimes for profit
 - Through scanning the network, a system is identified with a service containing a known vulnerability that can be exploited through a macro in a PDF document
 - Through advertisements, it is discovered that the company has a job out on tender
 - Through LinkedIn, a relevant contact person for the tender is discovered who probably has good system access

CKC Step 2. Weaponization

- The threat actor constructs exploit malware in a suitable format that can be delivered to the victim
- For example, can exploit one or more known vulnerabilities or zero-day vulnerabilities
- Example:
 - An exploit for the given vulnerability is created and integrated into a PDF file that will imitate a real tender for the job.

CKC Step 3. Delivery

- Malware that was developed is handed over to the target of the attack
- Could be through a USB, web server, phishing, or other attack vectors

CKC Step 3. Delivery: Through attack vectors



CKC Step 3. Delivery

- Skadware som ble utviklet overleveres til målet for angrepet
- Kan f.eks. være gjennom en USB, webtjener, phishing eller andre **angrepsvektorer**
- Eksempel:
 - En spear-phishing epost som later som å være fra en tidligere brukt leverandør opprettes
 - Sendes til identifiserte kontaktperson med PDF som vedlegg

CKC Step 4. Exploitation

- Execution of exploit on the vulnerability in the target system.
- Example:
 - The recipient opens the email
 - It looks real so they open the PDF to see its content
 - This causes the exploit to execute

CKC Step 5. Installation

- Malware is installed on the system
- A common effect of running the exploit is to open some form of access point (e.g., a backdoor) in the form of a command and control (C&C) channel the attacker can use.
- Now, the attacker has remote access to the infected system.
- Example:
 - The exploit is executed and used to install itself on the system and opens a backdoor back to the attacker
 - Attacker can now access the target's systems through the C&C channel

CKC Step 6. Command and Control (C&C)

- The attacker can explore the network around the infected system, propagate to other systems (lateral movement), hide traces and identify resources that can be stolen/sabotaged/exploited.
- Communication with attacker through created C&C channel
- Example:
 - In this example, the target was specific information
 - The attacker searches through the network to identify relevant information and hides their tracks along the way

CKC Step 7. Actions on Objective

- The actual goal of the attack is carried out
- This can be data mining, which means that data is collected, provisioned, and sent out of the network to servers controlled by attackers
- It can also be sabotage, in which case destructive actions are implemented.
- Example:
 - The attacker has now found relevant documents.
 - There are so many and they are large that these are transmitted over a long period of time to avoid this being detected
 - This is done through a hidden channel against Facebook
 - Afterwards, all traces of the extraction are deleted from the system

Detection Maturity Level (DML) model (Stillions)

Intelligence Categories

Detection Levels

Characteristics

Strategic: Attack strategy and objectives

DML-9

Attribution

DML-8

Goals

DML-7

Strategy

DML-6

Tactics

DML-5

Techniques

DML-4

Procedures

DML-3

Tools

DML-2

Host & Network Artifacts

DML-1

Atomic Indicators

DML-0

Undetected

Tactical/operational: Attack methods

Technical: Technical indicators of attacks

Analysis and enrichment

General and
long-term
intelligence

Detailed and
short-term
intelligence

Detection Maturity Level

- The DML model states that it is relatively easy to detect technical indicators such as IP addresses, domain names, and file names of malware, because it can be read directly from the logs, i.e. it only requires low maturity in incident response and digital threat intelligence.
- It requires greater maturity for an organization to be able to detect which **tactics, techniques and procedures** a threat actor has used in an attack, because these aspects cannot be read directly from the logs.
- It takes even greater maturity to be able to understand the attacker's underlying **strategies** and to be able to **attribute** an attack to a specific group. Detection of information extraction tactics (MITRE ATT&CK Exfiltration) or sabotage tactics (MITRE ATT&CK Impact) will indicate the attacker's objective.

APT – Advanced Persistent Threat

- A term that is often used in connection with the illustrated example is APT.
- An APT (Advanced Persistent Threat) is a threat actor or grouping.
- Often belongs to, or is often sponsored by, nation-states.
- There are also criminal APTs without such ties to nation-states.
- An APT must be seen as a grouping with an activity profile.
- Cyber operations by APTs typically target countries and sectors (e.g., defense, finance, industry, health, energy, ...).

APT – Advanced and persistent threat

- An APT is **Advanced** because it has at its disposal plenty of resources for intelligence, expertise and development of exploits to control infrastructures and carry out attacks.
- An APT is **Persistent** because it has long-term goals – often set by overarching political or strategic entities.
 - Means that it is persistent and cannot be stopped by resistance
 - Has the patience to perform attacks at a slow pace
 - Goes under the radar and harder to detect
 - Cyber operations can last for several years
- An APT is a **Threat** because it has purpose, opportunity and capability.

Description of APTs - examples

MANDIANT

APT1
Exposing One of China's Cyber
Espionage Units

Recorded Future

CYBER THREAT ANALYSIS

APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign

Intrusions Highlight Ongoing Exposure of Third-Party Risk

By Insikt Group
Co-Authored by Rapid7



CTA-2019-0206

- <https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units>

MITRE ATT&CK

- MITRE is a US (non-profit) organization. Through research and development activities, they support mainly US organizations at various levels, in both the public and private sectors, including academia.
- MITRE ATT&CK is a knowledge base that structures tactics and techniques used by attackers and various APT groups
- Contains mapping of different APT groups with techniques observed by them
 - *Note: the focus is on American/Western interests and MITRE ATT&CK does not contain, among other things, the NSA, which is very active in offensive cyber operations*
 - *They are because they are not considered a threat to US- interests*
- Based on observations of actual events
- An important part of the framework is the ATT&CK matrix with several associated projects. Can be used as a basis for threat modelling

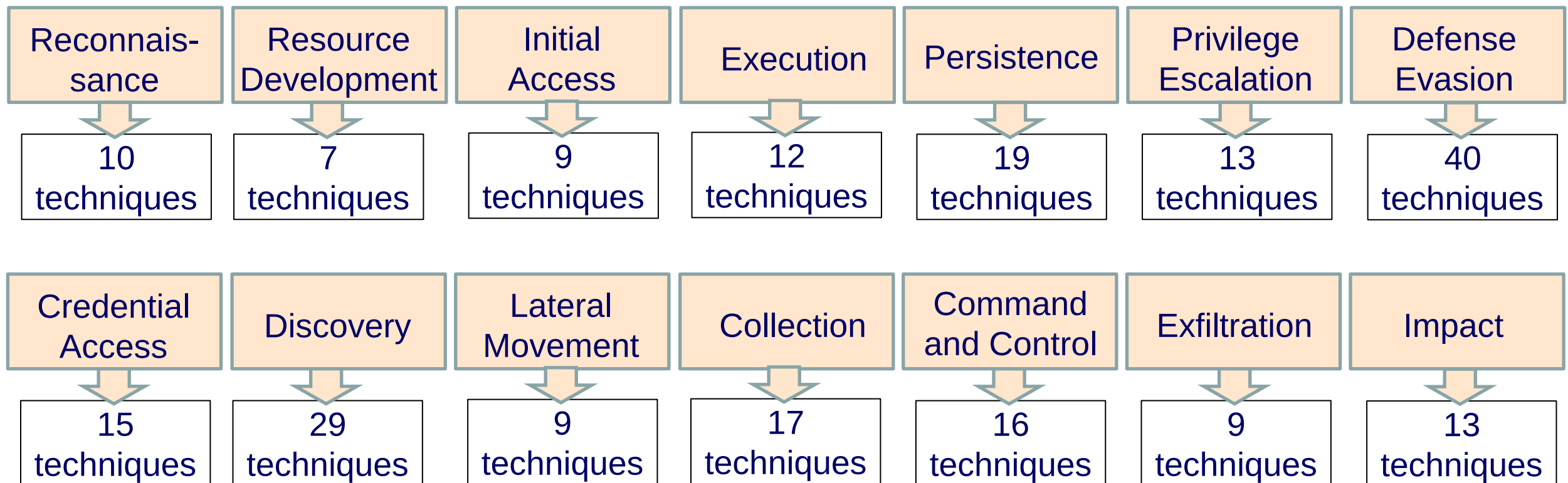
The MITRE ATT&CK Matrix

- The ATT&CK matrix is structured around techniques and tactics
- A technique represents **how** an attacker achieves a **tactical** objective through performing an action.
 - This could be, for example, phishing to gain access to a system.
 - A technique can be divided into part/under techniques
- A **tactic** represents **why** a technique is performed, in other words, a (sub)goal for the attacker.
 - For example, "access to system" is a tactic.
- In the ATT&CK matrix, each column is a tactic with techniques listed below them.

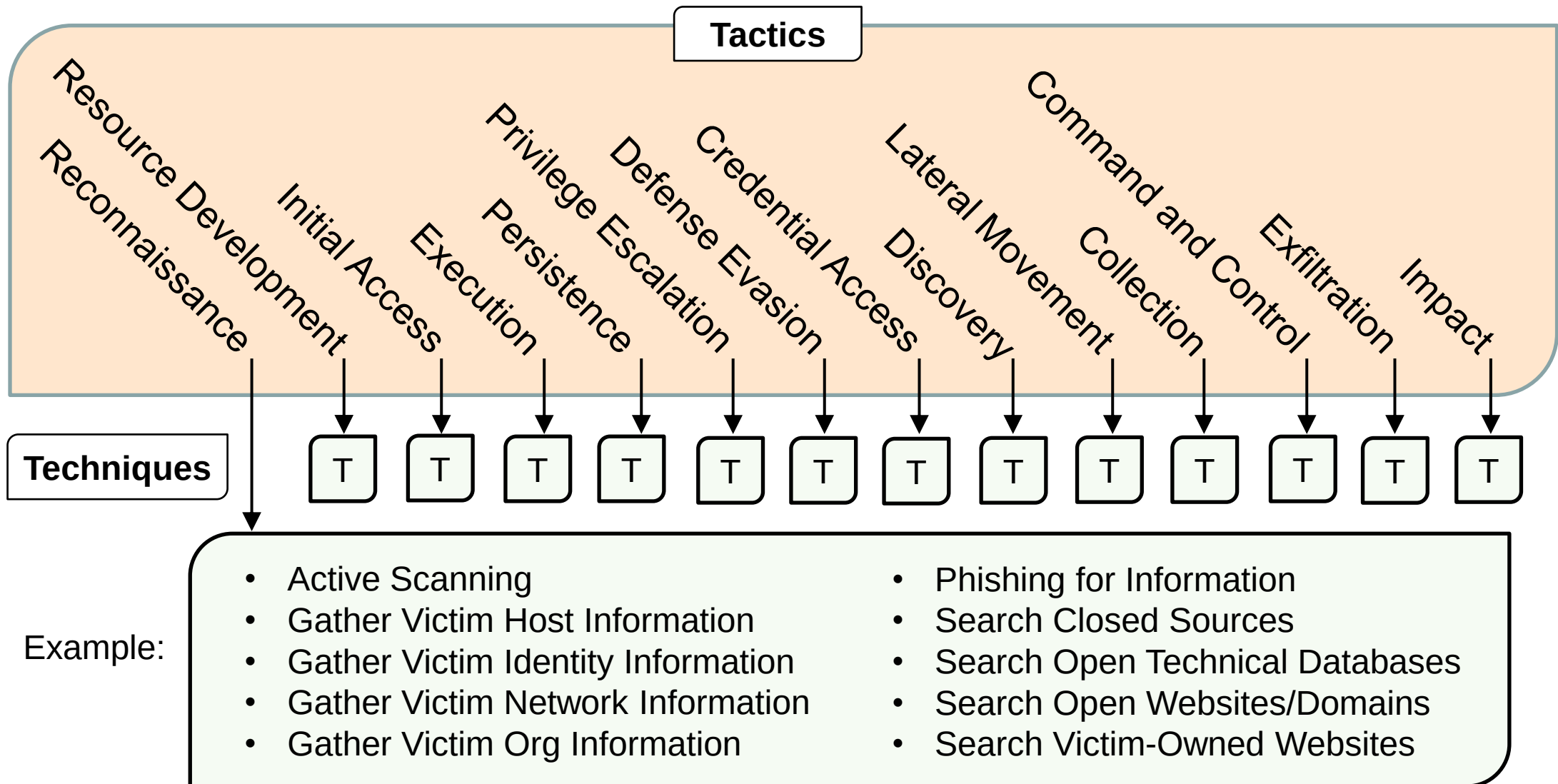
<https://attack.mitre.org/>

The MITRE ATT&CK Matrix

For each of the 14 tactics (sub-goals), various techniques are specified that attackers typically use to achieve the (sub-)goal.



<https://attack.mitre.org/>



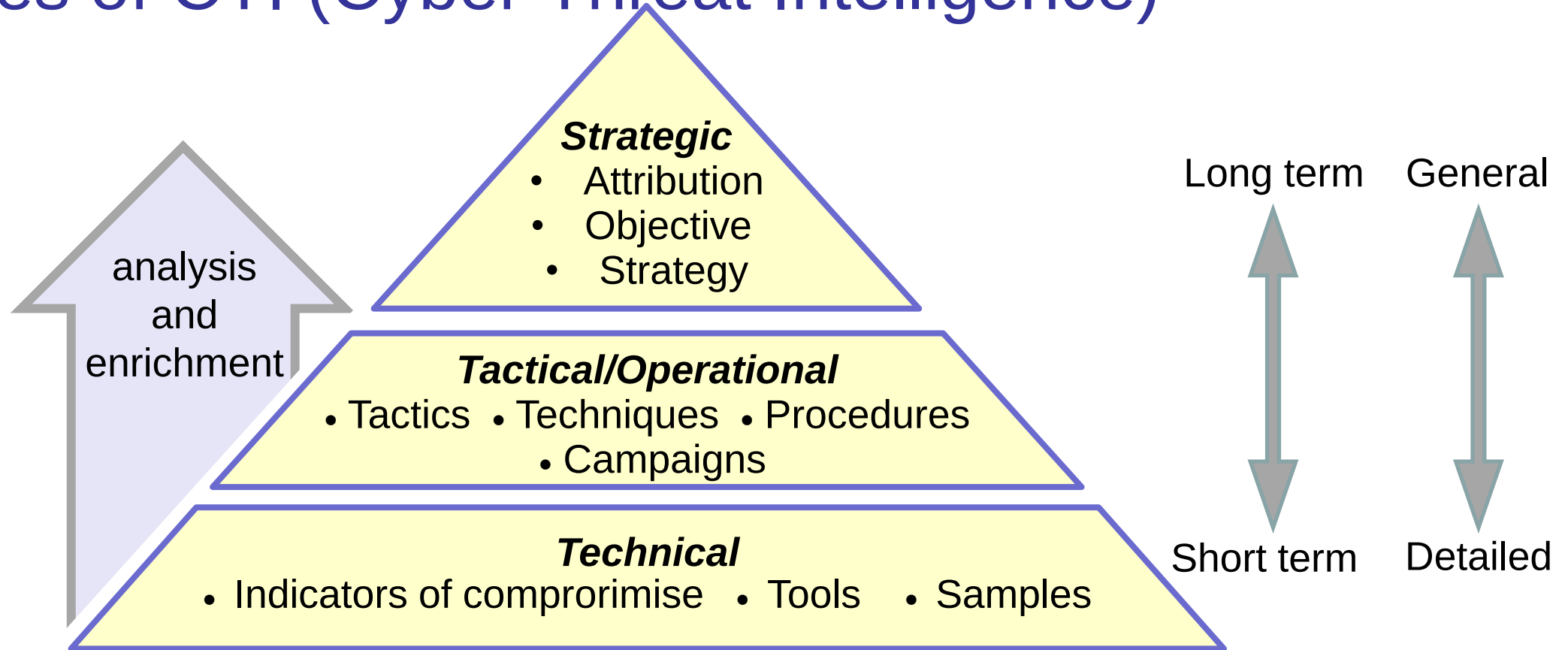
MITRE ATT&CK and APTs

[<https://attack.mitre.org/groups/>]

- Overview of different groups/APTs, as of today info on 152 groups
- Map each APT to observed techniques in the ATT&CK array

ID	Name	Associated Groups	Description
G0073	APT19	Codoso, C0d0so0, Codoso Team, Sunshop Group	APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same.
G0007	APT28	SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127	APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004. APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. In 2018, the US

Categories of CTI (Cyber Threat Intelligence)

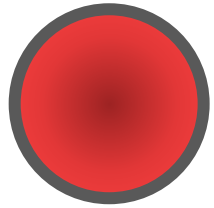


- CTI can be roughly divided into the three hierarchical categories: technical, operational, and strategic CTI.

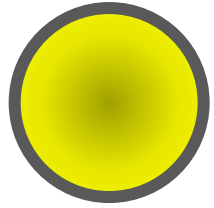
CTI categories

- **Strategic CTI:** Description of a threat actor/APT based on observed activities and other intelligence, as well as understanding the overall objectives and strategies of the threat actor. Attribution means that a CTI entity is able to identify which group is behind an attack. Strategic CTI is important for better positioning and prioritizing resources in defense against the threats.
- **Tactical/Operational CTI:** Information about which tools and tactics, techniques, and procedures (TTPs) are used in an attack. The term TTP can be interpreted as the way in which the threat actor carries out an attack, or as an "attack recipe". A threat actor usually has a limited selection of such attack recipes (TTPs) that they master and are used to using.
- **Technical CTI:** Indicators of compromise on attacks, which typically come from monitoring and logging activities in systems and networks. Attack indicators include, for example, IP addresses, domain names, signatures (hashes) of observed malware, and observed use of specific tools.

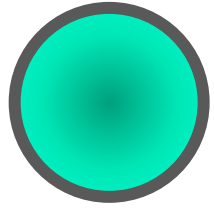
The Traffic Light Protocol (TLP) for Sharing CTI



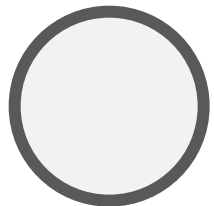
- **TLP-RED:** In person, for named recipients only. For example, during meetings between professionals, RED information is limited to those who are present. The distribution of RED information usually goes to a fixed list, and in extreme circumstances only verbal or personal handover.



- **TLP-AMBER:** Limited distribution, the recipient can share AMBER information with others in the organization and partners, but only on a "need-to-know" basis. The sender can specify the intended recipients in a detailed manner. **TLP-AMBER+STRICT** limits the sharing of CTI to only take place within one's own organization.



- **TLP-GREEN:** Within the sector, can be widely circulated within a specific environment. However, the information cannot be published or posted publicly on the internet, nor can it be forwarded outside the environment.

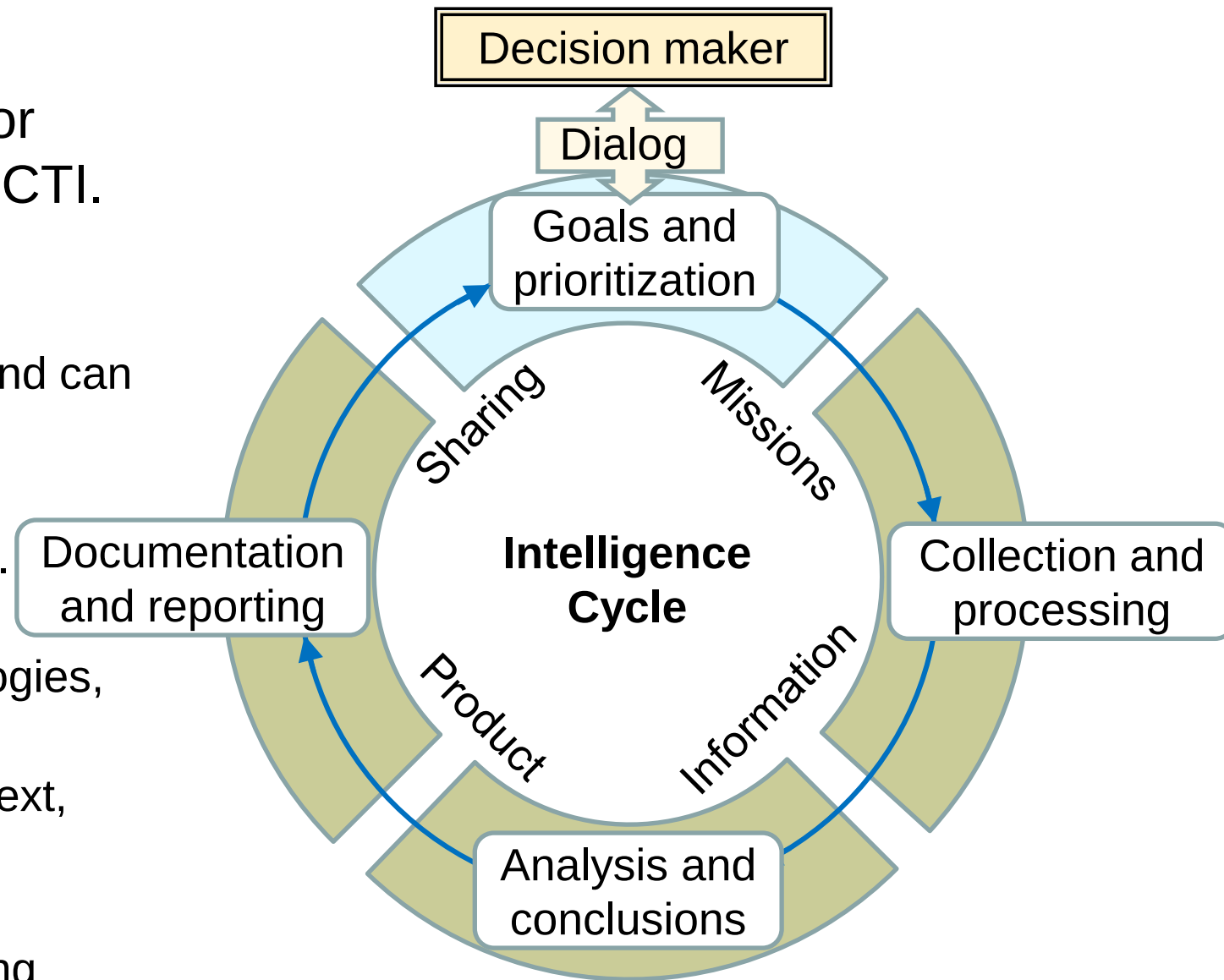


- **TLP-WHITE:** Unlimited, can be distributed freely, without limitation.

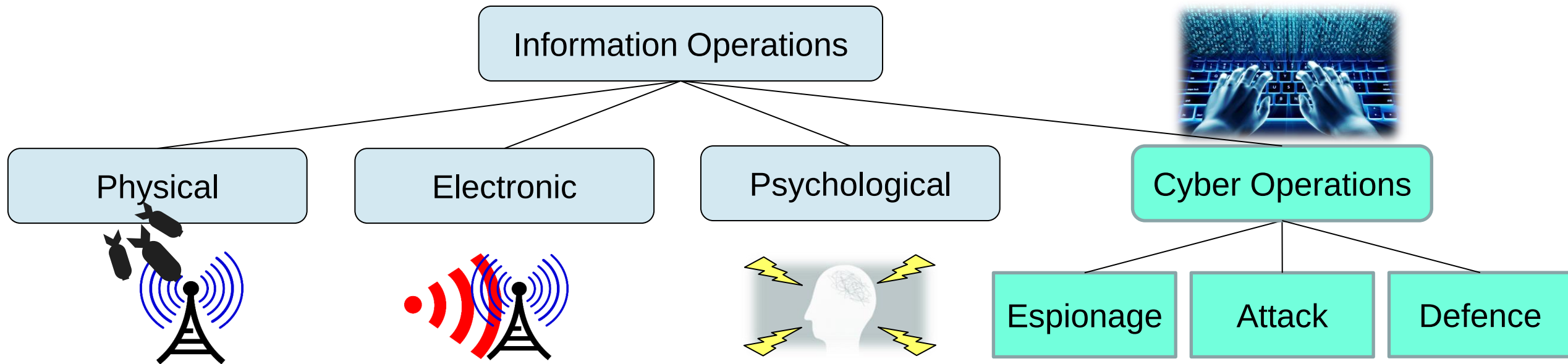
CTI Cycle

The intelligence cycle was defined for military intelligence; is also used for CTI.

- Threats can be directed at a business, a sector, or an entire state.
- Sources can be manual or automated, and can be internal or external.
- Data collected must be quality assured.
- CTI must be useful for making decisions.
- Analysis can be done with AI (artificial intelligence) or logical-semantic technologies, for example.
- Traditionally, CTI is articulated as plain text, and shared as pdf documents with other entities, but this scales poorly.
- Platforms for automated sharing are being developed based on machine-readable CTI.



Information Warfare



Cyber operations, aka. Computer Network Operations



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



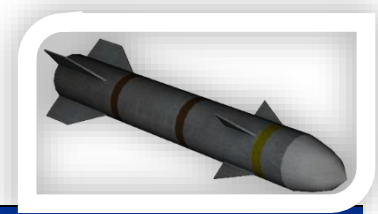
- Cyber Operations
US Cyber Operations Policy
 - Cyber Collection
 - Offensive Cyber Effects Operations (OCEO)
 - Defensive Cyber Effects Operations (DCEO)

Attribution of adversarial cyber operations

- The fog of cyber warfare
 - Difficult to find links to underlying power and its objectives for a cyber operation
 - Typically several hypotheses about identity and intention for a cyber operation.
 - Incorrect attribution of attacks can cause unintentional (political) damage
- Reverse engineering of cyber attacks
 - Based on analysis of observed indicators, and CTI (Cyber Threat Intelligence)
 - Attribution and understanding the intent of attacks
 - Challenging because
 - Attacks can be channeled through multiple channels and nodes to confuse back-tracking
 - Deliberate misrepresentation of attack indicators
 - Difficult to understand intention based on observed activity



Comparison between cyber and kinetic



Property	Cyber weapons	Kinetic weapons
Harmful effect	Harms CIA in IT systems and affects processes that depend on IT systems. May affect far more actors and sectors than the attack was aimed at. May cause indirect physical damage to cyber-physical systems.	Kinetic weapons cause direct physical damage to infrastructure. Only affects the area where the weapon hits.
Reuse	Can be reused/recycled through malware reverse-engineering, so that the victim can reuse the cyberweapon to attack others.	Kinetic ammunition is destroyed in the attack, can only be used once.
Openness	Cyber weapons are immaterial, and thus easy to hide. Cyber weapons are usually kept hidden because transparency would make it possible to develop countermeasures that render the weapon useless.	Kinetic weapons are often physically large, and thus visible, e.g. from satellites. Transparency does not necessarily weaken the weapon.
Attribution	It is often challenging to identify which group or state is behind cyberattacks. The threat actor can leave misleading traces to frustrate attribution.	It is usually relatively easy to see where a kinetic attack is coming from, thus attributing to an actor.
Durability	Cyber weapons are often based on zero-day vulnerabilities that have a limited shelf life, often less than a year. CyberOps actors therefore need a continuous supply of new cyber weapons.	Kinetic weapons have a long shelf life, typically decades. Large arsenals of weapons can be stored for a long time.

The Usefulness of Cyber Espionage and Offensive Cyber Operations

Cyber espionage

- Provides great advantages for intelligence gathering
- Cheaper and less risky than traditional physical espionage

Offensive cyber operations

- Can paralyze digital systems and processes
- Attacks against critical infrastructure can be particularly damaging
- Consequences can be reduced by good emergency preparedness and incident management
- Attackers must have significant resources to achieve significant impact
- Often cheaper to get the same effect with physical attacks
- Attacker has the advantage of difficult attribution

Offensive cyber operations combined with physical operations

- Observert bruk av cyberoperasjoner i nåværende konflikter (Ukraina)
- Ansett for å være svært nyttig sammen med fysiske militæroperasjoner.
- Forvirrer og forstyrrer fienden når kommunikasjon og koordinering er mest kritisk

Countries with official cyber operations strategy

- Military defense strategies in the 21st century must necessarily include a strategy for cyber operations.
- The United States has a clearly expressed official policy on cyber operations.
- Other countries may reason that cyber weapons are invisible, and that it is an advantage not to publish a strategy for cyber operations.



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

<https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html>

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



Cyber deterrence



- Russia has compromised power grids in Western countries since 2014
 - Reports of Compromise and Spying on Power Grids in the United States
 - Sabotage against Ukraine in December 2015
- The US has been compromising power grids in Russia since 2018
 - How do we know? Article in the New York Times:
<https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>
 - Why? To deter.

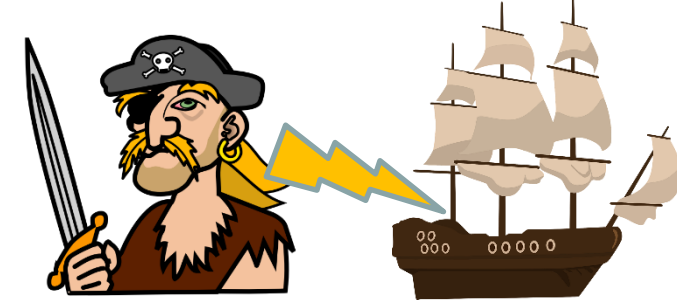
U.S. Escalates Online Attacks on Russia's Power Grid



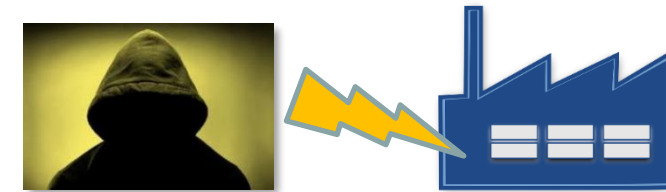
A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections. *Maxim Shemetov/Reuters*

Cyber Privateering

- Privateering in the period 1600 – 1850 was legalized piracy.
 - The pirates were given a “*letter of marque and reprisal*”
- Russian President Putin has stated that Russian groups that carry out cyber attacks against other countries are not considered criminals, "because they do not violate Russian law."
 - Russian hacker groups thus have letters of marque and reprisal.
- The Paris Call for Trust and Security in Cyberspace (2018) failed because the major powers want to be able to carry out cyber operations, and because compliance with a treaty would be difficult to enforce.
- In 2024, the UN proposed a treaty against cybercrime.



Privateering 1600 - 1850



Cyber Privateering 2020→



Cyber Warfare and Big Tech

- On Wednesday, February 23, 2022, a few hours before Russian tanks began rolling into Ukraine, Microsoft's Threat Intelligence Center found indicators of a never-before-seen "Wiper" malware being used in attacks against Ukraine's government ministries and financial institutions.
- The Microsoft Threat Intelligence Center quickly picked apart the malware, named it "FoxBlade" and alerted Ukraine's top cyber defense authority.
- The FoxBlade malware is programmed to wipe all data on a computer that is available in a computer network.
- Within three hours, Microsoft's virus detection systems on Windows servers had been updated to block FoxBlade.



Yanukovych and Putin



Petro Poroshenko



Volodymyr
Zelenskyy

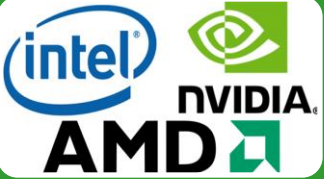


Potential for collaboration with Big Tech



OS Vendors

- Software updates and regular patching
- Potential total control over all systems onlineers



CPU and microchip producers

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



Computer manufacturers

- Configures boot, can embed spyware during production
- Monitoring and control of computer platforms during operation



Cloud providers

- Passive or active access to IaaS, PaaS, and SaaS
- Monitoring and governance in the cloud



Internet infrastructure providers

- Major telcos, DNS and AS (Autonomous System) operators, Internet routing
- PKI root CA operators, basis for cryptographic security on the Internet

Where is cyber warfare going?

- Lack of international rules for cyber operations
- Cyber warfare affects all organizations
- Global problem
- Big Tech plays an important role
- Rapid innovation
- Unpredictable future

