CYBER SECURITY IN CONSTRUCTION AND PROPERTY MANAGEMENT

Aapo Cederberg
24.8.2023

CWF
Cyberwatch Finland

CYBER SECURITY IN CONSTRUCTION AND PROPERTY MANAGEMENT

1. ***Challenges and threats***
2. Practical examples
3. Improving cybersecurity

Cyberwatch Finland

1. Challenges and threats

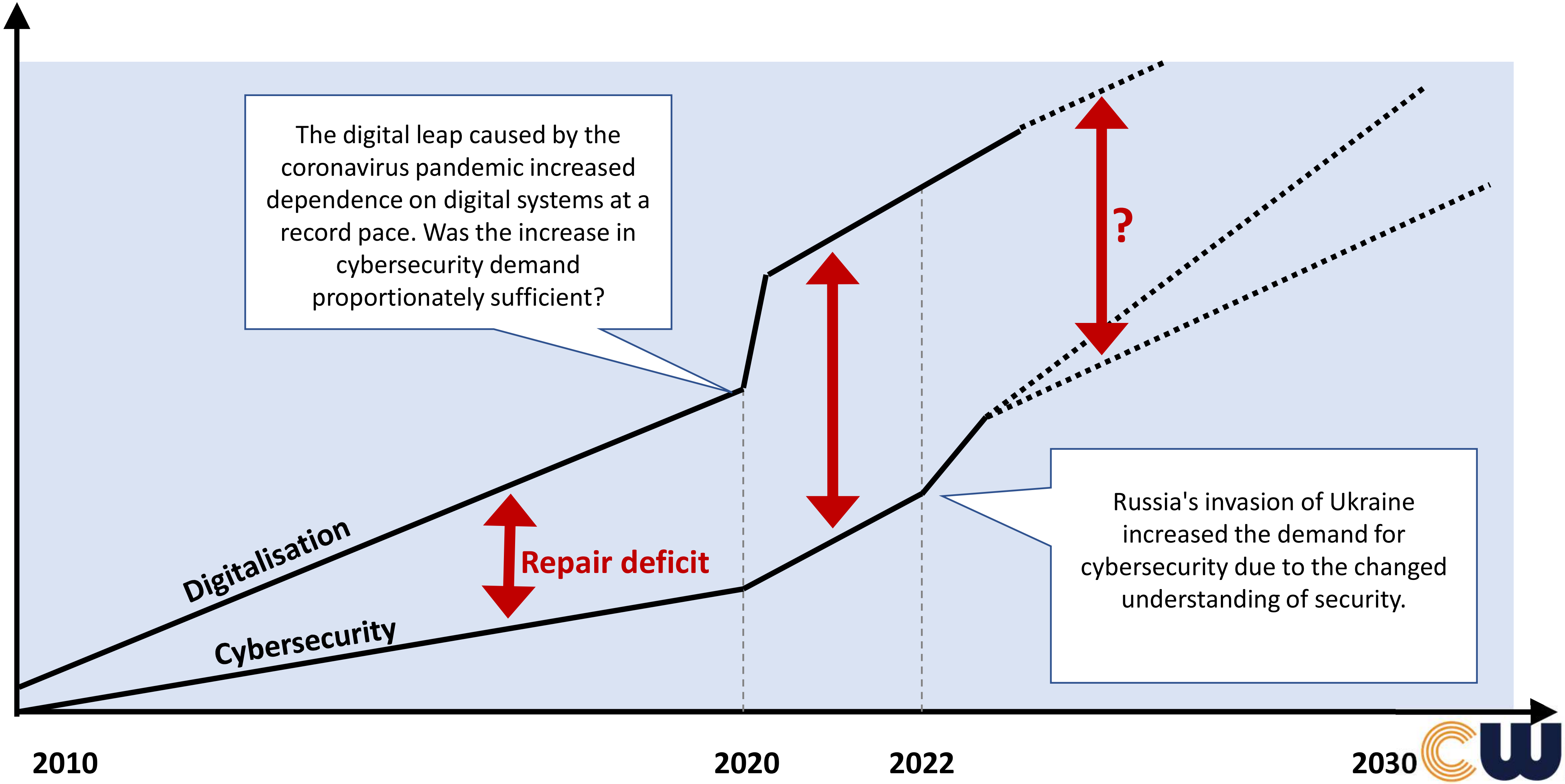
THE RISKS AND CHALLENGES OF THE DIGITAL OPERATING ENVIRONMENT ARE INCREASING!

- **Digitalisation is commonplace, regardless of the industry**
- Digitalisation expands the company's operating environment and results in new threats and risks that must be identified and handled
- What is the scope and criticality of digital and networked (business) operations for a company?
- The objective of cybersecurity is to secure operations dependent on a disrupted cyber environment.
- Increasing demands on corporate cybersecurity
    - For example, in consumer products: the proposed EU Cyber Resilience Act, information security requirements apply to devices and software connected to a data network
    - In business services and operations: NIS2 Cybersecurity Directive (key actors: healthcare/important actors: medical devices, machinery and devices; monitoring, reporting, sanctions)

Cyberwatch Finland

1. Challenges and threats

DIGITALISATION VS DIGITAL SECURITY



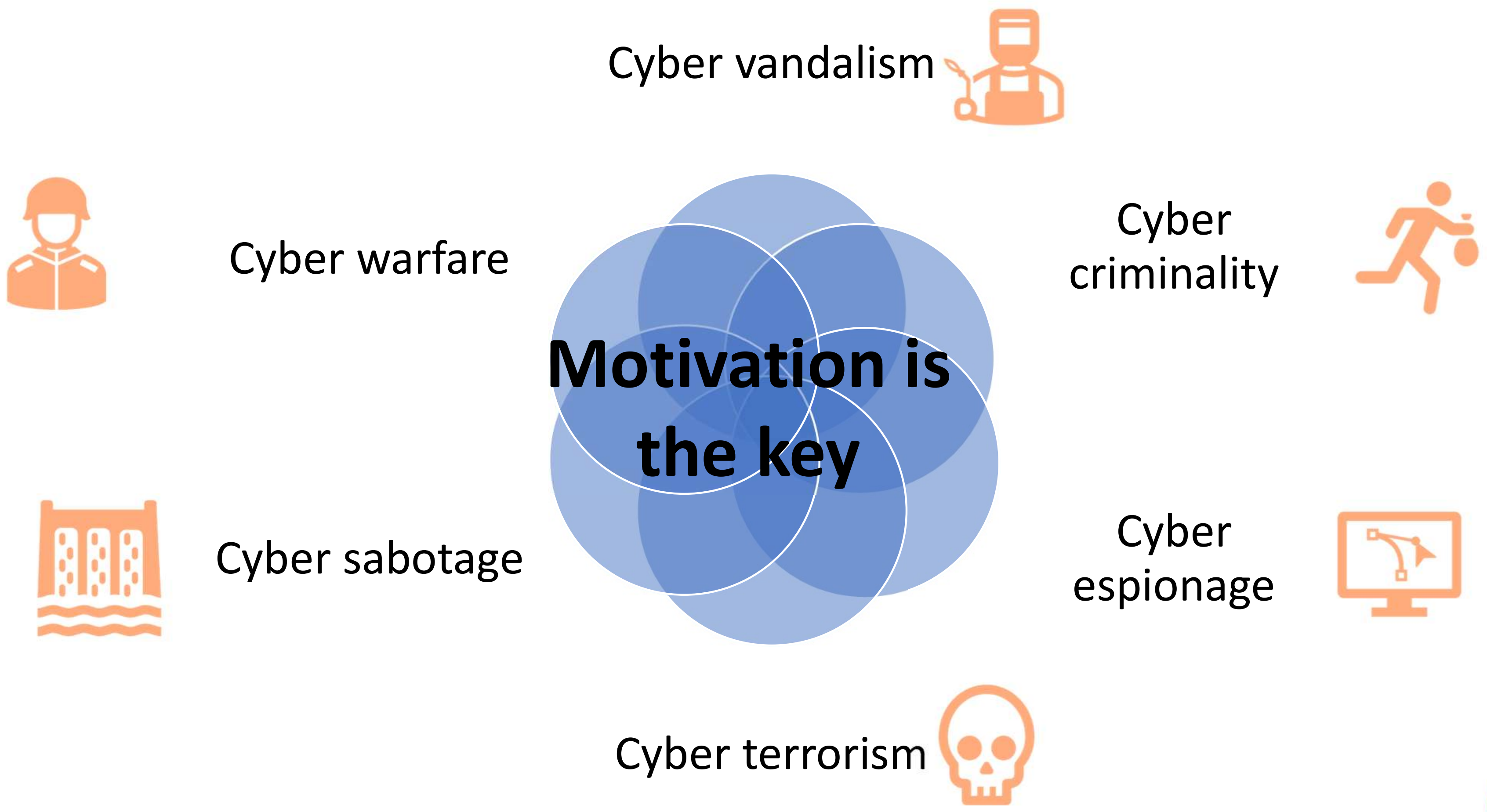
The digital leap caused by the coronavirus pandemic increased dependence on digital systems at a record pace. Was the increase in cybersecurity demand proportionately sufficient?

Russia's invasion of Ukraine increased the demand for cybersecurity due to the changed understanding of security.

Cyberwatch Finland

1. Challenges and threats

CYBER THREAT ENVIRONMENT



Cyber vandalism

Cyber warfare

Cyber criminality

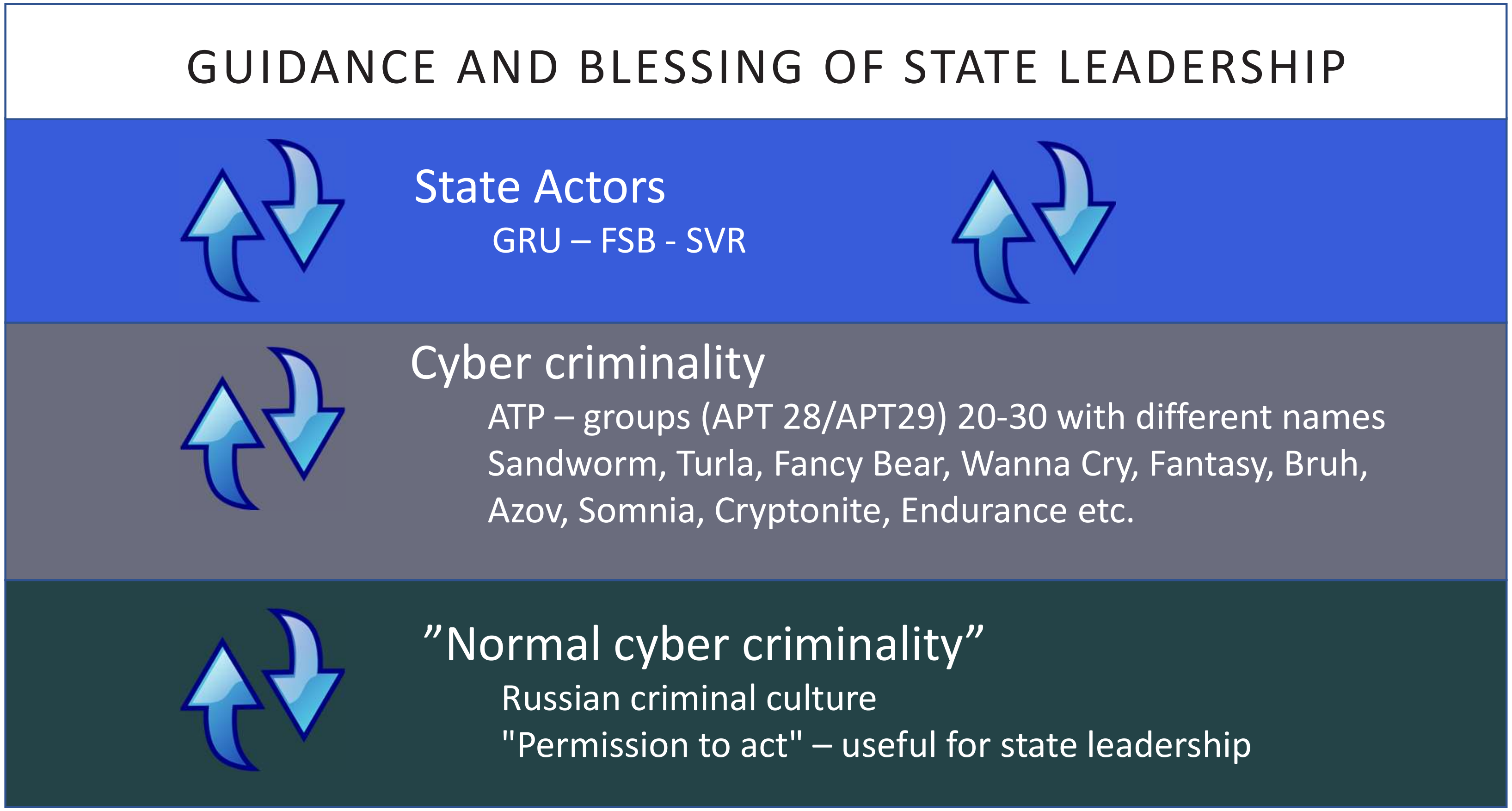
Motivation is the key

Cyber sabotage

Cyber espionage

Cyber terrorism

RUSSIAN CYBER POWER



GUIDANCE AND BLESSING OF STATE LEADERSHIP

State Actors

GRU – FSB - SVR

Cyber criminality

ATP – groups (APT 28/APT29) 20-30 with different names
Sandworm, Turla, Fancy Bear, Wanna Cry, Fantasy, Bruh,
Azov, Somnia, Cryptonite, Endurance etc.

”Normal cyber criminality”

Russian criminal culture
"Permission to act" – useful for state leadership

Cyberwatch Finland

1. Challenges and threats

RUSSIAN CYBER THREAT

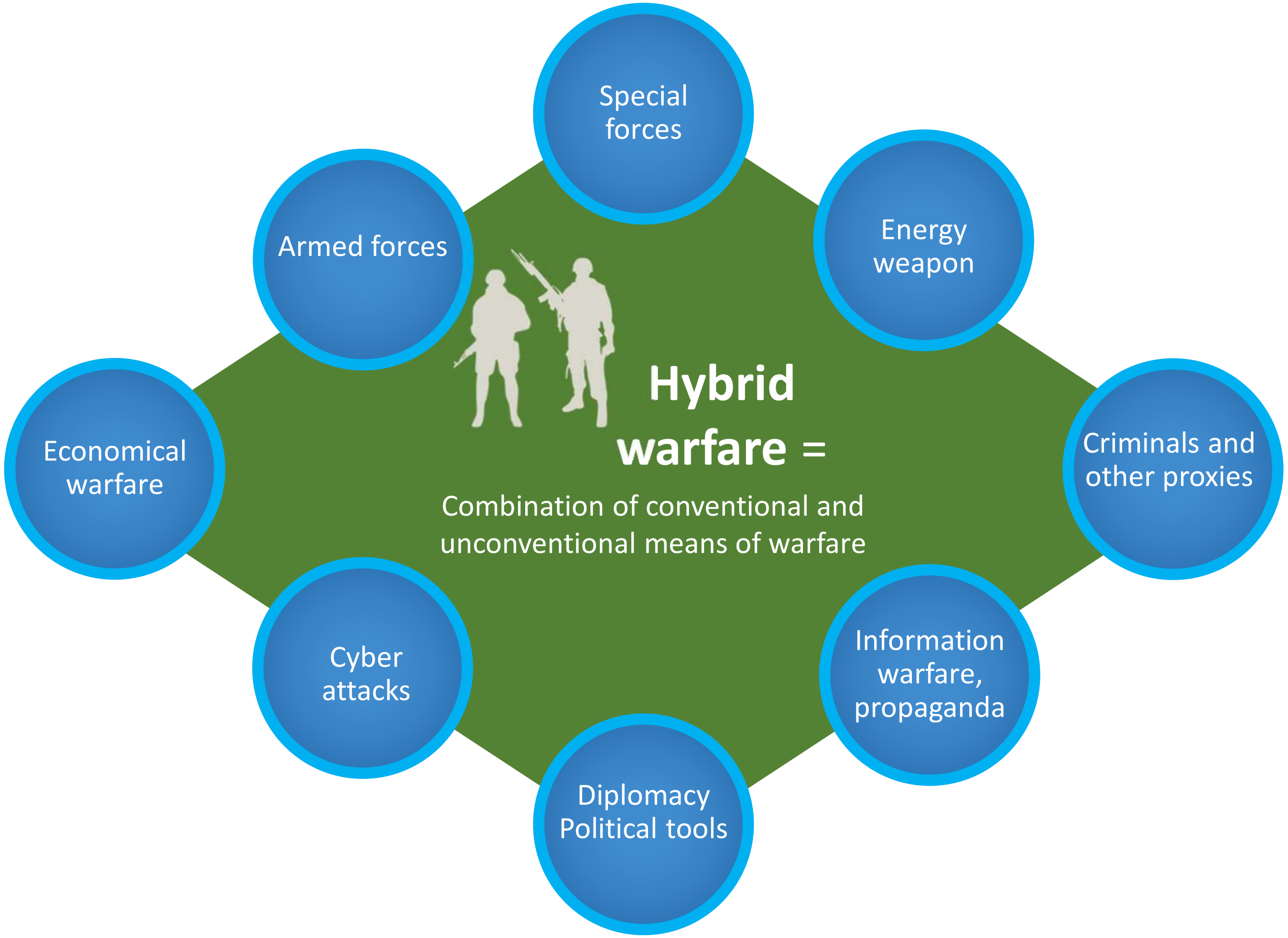
Aleksander Bartosh, the leading Russian expert on hybrid warfare today, wrote in 2018 in the journal of the Russian General Staff that the biggest change in the transition from the Cold War to hybrid warfare was the shift from a struggle between ideologies to a struggle between civilisations.

In Russia's view, therefore, the current struggle is for the existence of civilisations and ideologies. The winner of such a war not only gains control of the defeated state and its resources, but also the right to decide on the loser's future.

From Russia's point of view, this is precisely a struggle between Western civilisation and Russia.

1. Challenges and threats

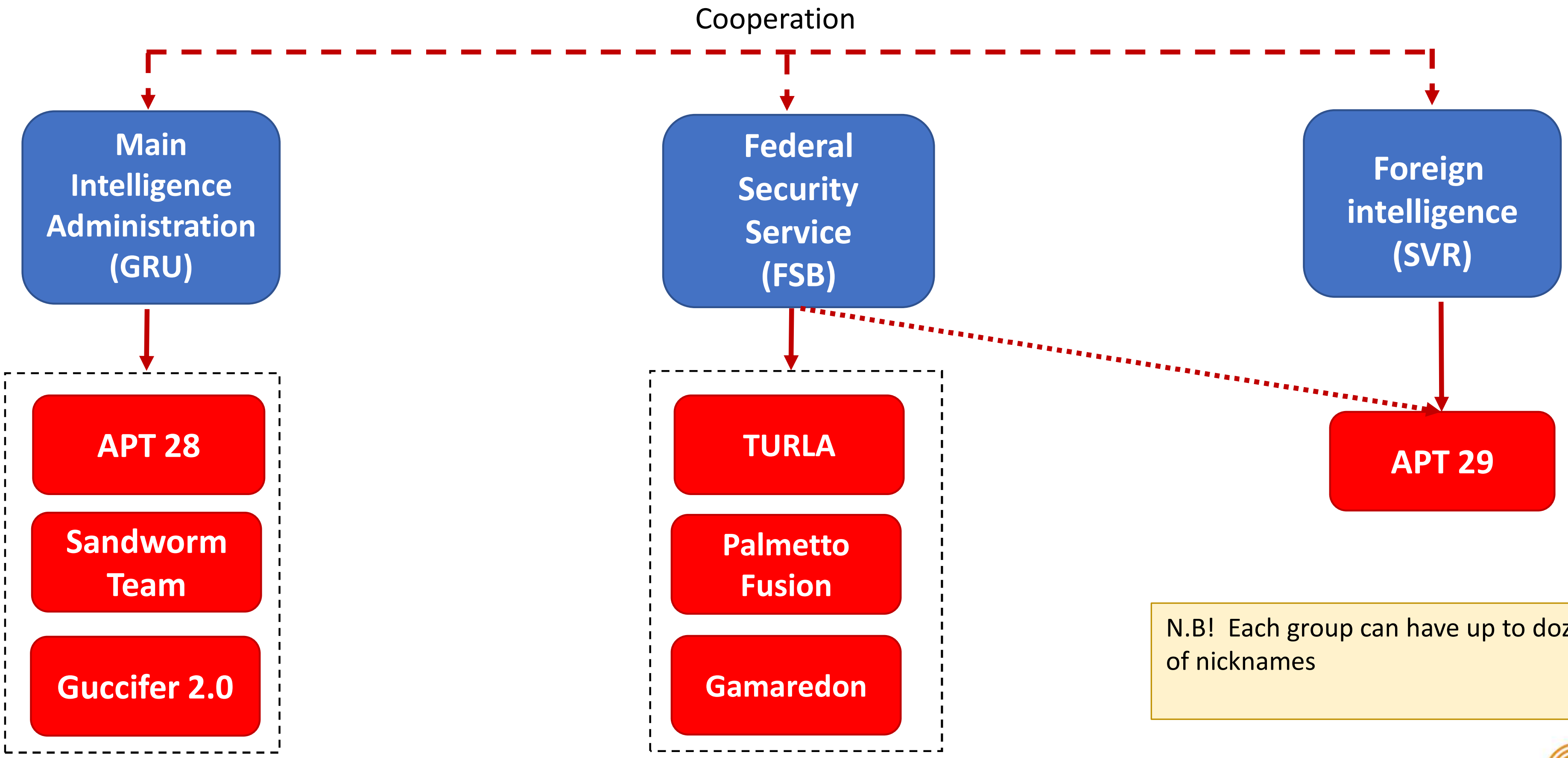
RUSSIAN HYBRID WARFARE


Special forces
Armed forces
Energy weapon
Economical warfare
Hybrid warfare =
Combination of conventional and unconventional means of warfare
Criminals and other proxies
Cyber attacks
Information warfare, propaganda
Diplomacy Political tools

Cyberwatch Finland

1. Challenges and threats

RUSSIA'S MOST PROMINENT HACKER GROUPS


Cooperation
Main Intelligence Administration (GRU)
Federal Security Service (FSB)
Foreign intelligence (SVR)
APT 28
Sandworm Team
Guccifer 2.0
TURLA
Palmetto Fusion
Gamaredon
APT 29

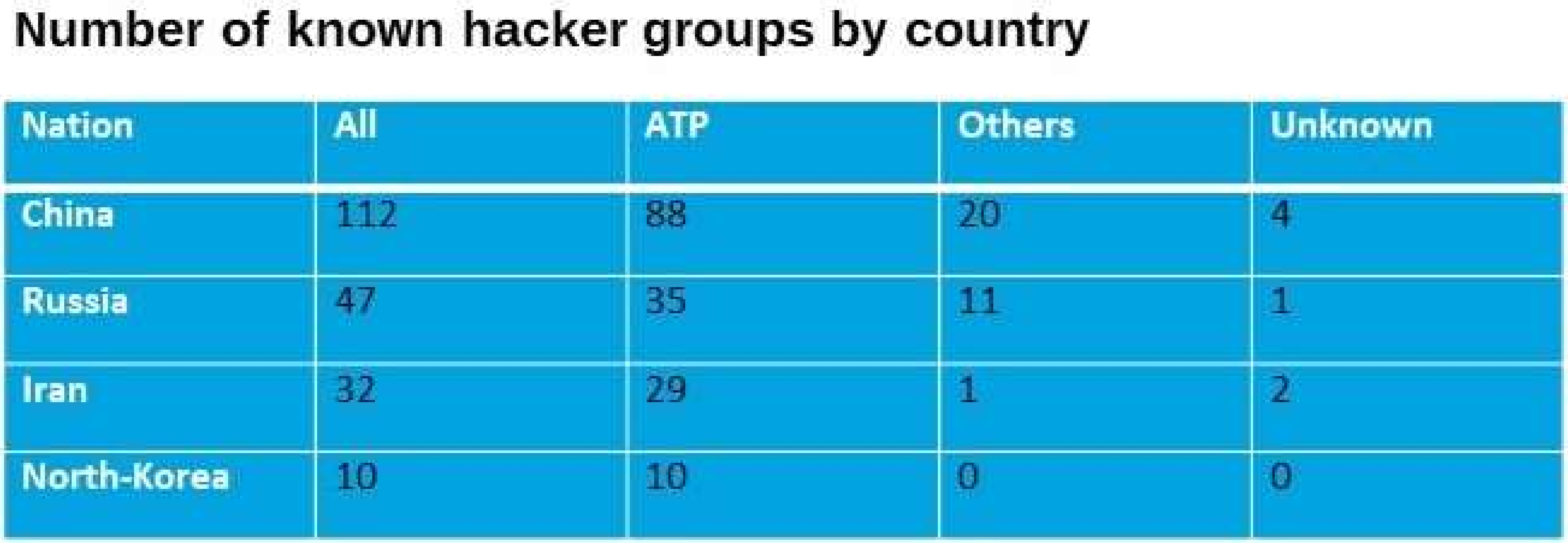
N.B! Each group can have up to dozens of nicknames

Sources: Cunningham, Conor: *A Russian Federation Information Warfare Primer*, Research report, University of Washington, 12.11.2020 *Russian Cyber Units*, Congressional Research Service, January 4, 2021

Cyberwatch Finland

1. Challenges and threats

RUSSIAN CRIMINAL CULTURE



Number of known hacker groups by country

Nation	All	ATP	Others	Unknown
China	112	88	20	4
Russia	47	35	11	1
Iran	32	29	1	2
North-Korea	10	10	0	0

1. Challenges and threats

CHINA´S ROLE

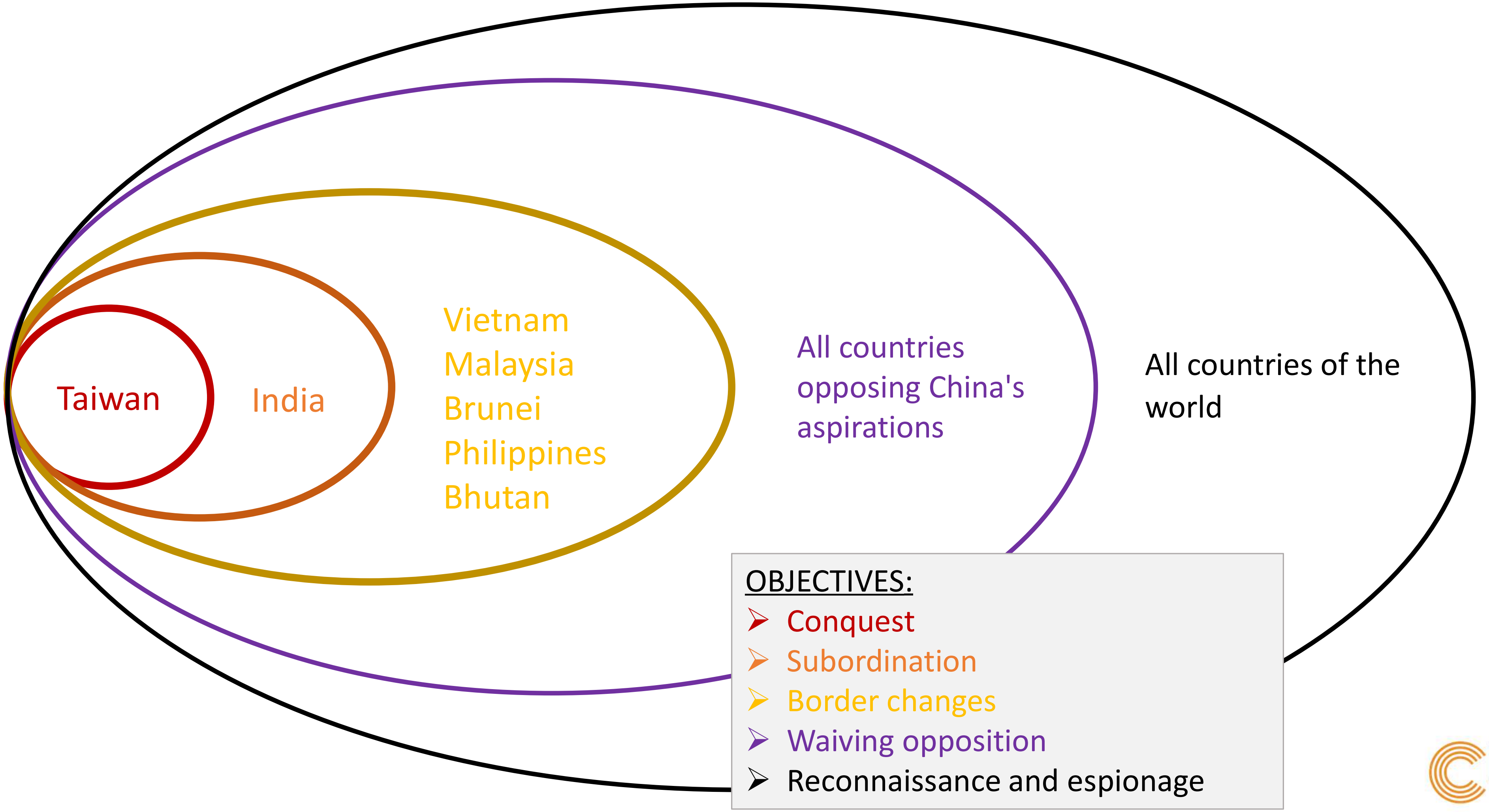
Over the years, China has become a major player in hybrid warfare, and despite Russia's reputation, China is probably the most significant country using hybrid warfare.

The same phenomenon exists for "state hacker departments" belonging to the APT category.

Although China operates on the broadest front, Russia's cyber activities gain the most visibility. The visual illusion is due to the Eurocentric view that naturally prevails in the European media.

1. Challenges and threats

TARGETS AND OBJECTIVES OF CHINA'S HYBRID WARFARE



Taiwan

India

Vietnam
Malaysia
Brunei
Philippines
Bhutan

All countries opposing China's aspirations

All countries of the world

OBJECTIVES:

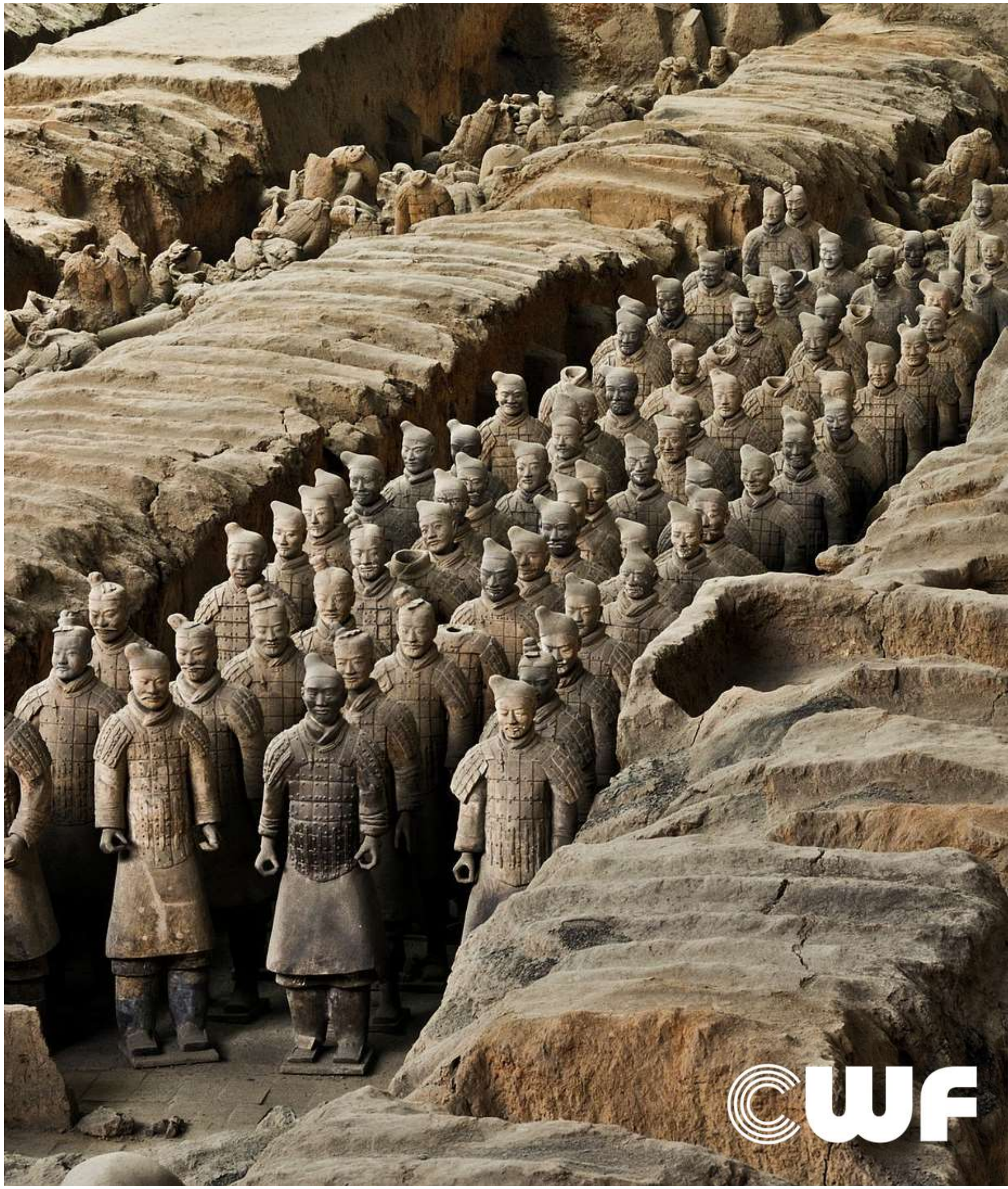
- Conquest
- Subordination
- Border changes
- Waiving opposition
- Reconnaissance and espionage

1. Challenges and threats

CHINA'S AMBITIONS

China can only wipe out the shame it has suffered by uniting all the territories it has lost through the following wars:

- China will invade and annex Taiwan in 2020-2025
- China will capture the Spratly Islands in the South China Sea between 2025 and 2030
- China will reconquer southern Tibet (Arunachal Pradesh region) between 2035 and 2040
- China will capture the Diaoyu and Ryukyu Islands in the sea between Taiwan and Japan between 2040 and 2045
- China will unite Outer Mongolia between 2045 and 2050
- China will reconquer the territories it lost to Russia between 2055 and 2060



OFFENSIVE CYBER DEFENCE

- The US is leading global development when it comes to offensive cyber operations. According to the new cybersecurity strategy, weakening of opponents' cyber capabilities is one of the main components of an effective cyber defence.
- Defend Forward – concept places itself somewhere in between passively defensive operations and aggressive and offensive actions. The aim of the strategy is the reinforce critical targets by increasing the costs of possible attacks and increasing the likelihood of the attacker getting caught.

OFFENSIVE CYBER DEFENCE

- Capabilities of developing cyber weapons and carrying out attacks vary greatly between NATO countries. NATO has developed its own strategy for carrying out offensive operations, and this allows for individual actions of singular states within the alliance.
- Cyberweapons and attacks have been used for long time, and they are becoming more and more visible in strategies regarding cybersecurity. In future, one cannot produce an effective cyber defence without the capability of offensive actions. This development increases the pressure on countries whose development of offensive capabilities is in its infancy.

CER-DIRECTIVE – ”THE RESILIENCE DIRECTIVE”

- CER –directive (Critical Entities Resilience;) is also known as the resilience directive. Updated version of the directive (Directive on the Resilience of Critical Infrastructure) was accepted at the end of December of 2022.
- Member states have 21 months to adjust national laws to be in accordance with the directive. CER is based on EU's strategy of security, which stated that vital everyday used critical infrastructure must be secure and resilient.
- The scope of the directive covers eleven sectors. Sectors include transportation, energy, banking, finance, healthcare, drinking water and wastewater, food, digital infrastructure, public administration and space.

Cyberwatch Finland

NIS2 NETWORK AND INFORMATION SECURITY DIRECTIVE – CYBERSECURITY DIRECTIVE

The goal of NIS2 is to ensure shared high level of cybersecurity in the entire EU by increasing the resilience and reaction capabilities to cyber threats for both public and private sector.

"Technologies used in everyday life, of which we are dependent, must be secured against ever developing cyberattacks, regardless of whether they originate from EU or outside of it".

NIS2 SECTORS

ESSENTIAL ENTITIES

- Energy
- Transportation
- Banking, financial market infrastructure
- Healthcare
- Drinking water & wastewater
- Digital infrastructure
- Public administration
- Space

IMPORTANT ENTITIES

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing
- Digital providers
- Research

Cyberwatch Finland

CYBER SECURITY IN CONSTRUCTION AND PROPERTY MANAGEMENT

1. Challenges and threats
2. ***Practical examples***
3. Improving cybersecurity

Cyberwatch Finland

INDUSTRIAL AUTOMATION AS A TARGET

- Digitalisation makes it possible to access machinery systems and real estate data from anywhere in the world --> the same possibility exists for criminals!
- **Cyberattacks targeting automation and critical infrastructure have increased**
- Vast amounts of networked remote accessible automation and control systems are found in the open web and therefore also subject to attacks aiming to gain illicit entrance
- Nation-state sponsored cyberattacks have increased and by attacking industrial automation it is relatively easy to cause instability
- For example, a denial-of-service attack on an automation systems has the potential to override the electricity grid causing blackouts and outages

2. Practical examples

INDUSTRIAL AUTOMATION AS A TARGET

Information security on Finnish industrial automation has been lacking:

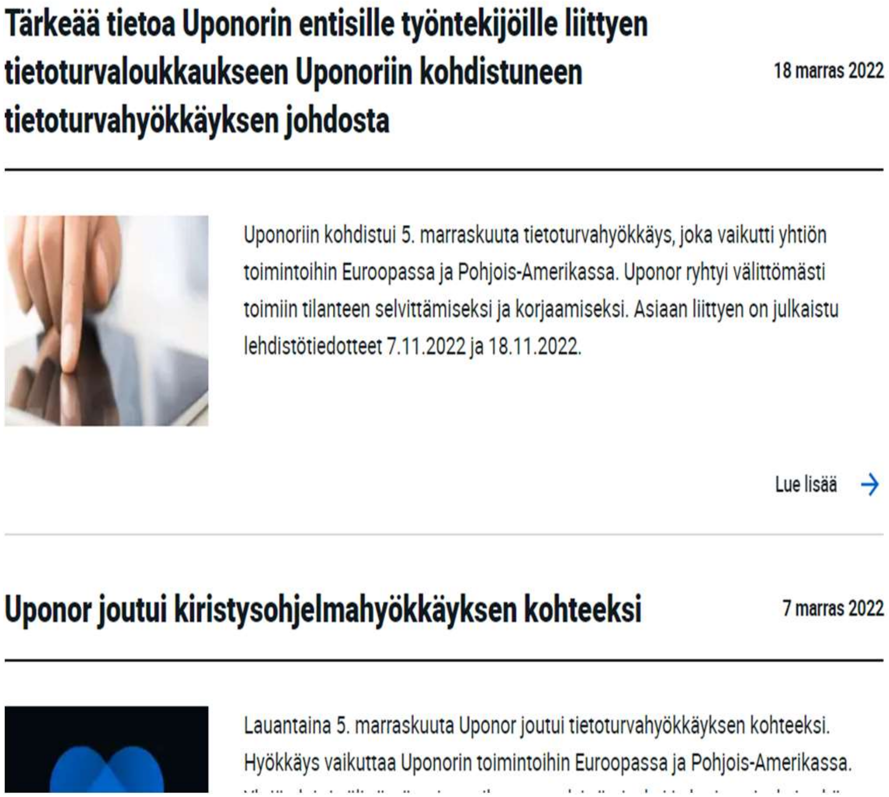
- A lot of open or insufficiently protected systems
- Risk management often lacking
- Quality or savings: Cheap price tag increases the number of vulnerabilities

Regular updates, preventing remote control, and changes in configuration decreases the risk of being targeted

CASE UPONOR

A Finnish company providing systems for construction and environmental technologies was targeted by a cyberattack on 5h of November 2022.

- **Attack vector:** Ransomware and a possible data breach
- **Effects**:
  - Spreading effects on company's operations in Europe and North America
  - Seizure of production lasting a week
  - Issued out a warning for investors due to uncertainty of abilities to recover from lost sales before the end of the year
  - Possible data breach concerns data belonging to clients, employees and partners
- **Attacker**: unknown
- **Company's reaction:**
  - As a precaution shut down of all systems and production
  - Begun immediate actions to understand and remedy the situation
  - Informed the authorities and data protection ombudsman



Tärkeää tietoa Uponorin entisille työntekijöille liittyen tietoturvaloukkaukseen Uponoriin kohdistuneen tietoturvahyökkäyksen johdosta 18 marras 2022

Uponoriin kohdistui 5. marraskuuta tietoturvahyökkäys, joka vaikutti yhtiön toimintoihin Euroopassa ja Pohjois-Amerikassa. Uponor ryhtyi välittömästi toimiin tilanteen selvittämiseksi ja korjaamiseksi. Asiaan liittyen on julkaistu lehdistötiedotteet 7.11.2022 ja 18.11.2022.

Uponor joutui kiristysohjelmahyökkäyksen kohteeksi 7 marras 2022

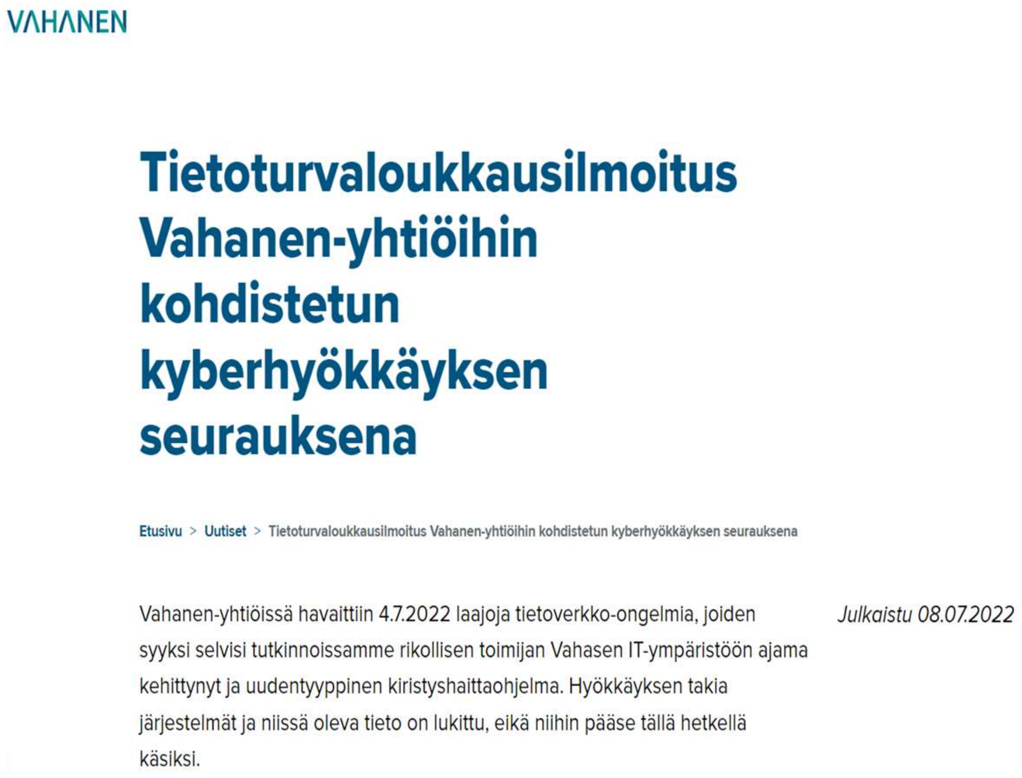
Lauantaina 5. marraskuuta Uponor joutui tietoturvahyökkäyksen kohteeksi. Hyökkäys vaikuttaa Uponorin toimintoihin Euroopassa ja Pohjois-Amerikassa.

CASE VAHANEN

Construction consultation company Vahanen observed wide disturbances on networks on July of 2022 cause of which revealed to be a cyberattack

- **Motive**: Financial or national?
- **Attack vector**: New type of ransomware
- **Effects**:
  - Lockdown of all company's data systems
  - Former and current employees had their data stolen in addition to project and personal data of customers and partners
  - Significant harm to many projects leading to delays

Attacker: Incident was a part of wider attempt to target multiple companies in Europe simultaneously --> attacker itself unknown



VAHANEN

Tietoturvaloukkausilmoitus Vahanen-yhtiöihin kohdistetun kyberhyökkäyksen seurauksena

Etusivu > Uutiset > Tietoturvaloukkausilmoitus Vahanen-yhtiöihin kohdistetun kyberhyökkäyksen seurauksena

Julkaistu 08.07.2022

Vahanen-yhtiöissä havaittiin 4.7.2022 laajoja tietoverkko-ongelmia, joiden syyksi selvisi tutkinnoissamme rikollisen toimijan Vahasen IT-ympäristöön ajama kehittynyt ja uudentyyppinen kiristyshaittaohjelma. Hyökkäyksen takia järjestelmät ja niissä oleva tieto on lukittu, eikä niihin pääse tällä hetkellä käsiksi.

2. Practical examples

THE SECURITY OF OPERATIVE TECHNOLOGIES (OT)

- Industrial networks have traditionally been isolated from internet and even from organisation's own IT-systems, and they have been operated by the staff of production facilities
  - This has previously guaranteed the security of these systems
  - Lately interests in remote control and boosting production have changed the forms of operation
  - OT systems are increasingly connected to internet and often lacking sufficient security systems
  - Integration of OT systems and internet has demanded forming new types of connections subjecting old and not updated systems to same threats and risks that are found in IT-environments

- Interesting and easy target from the perspective of a cyber attacker --> vulnerable systems --> significant effects
- Examples of attacks on OT-systems:
  - Cyberattack on Indian oil company (2022)
  - Colonial pipeline cyberattack (2021)
  - Dr Reddy’s laboratories cyberattack (2020)
  - Nuclear plant of Kudankulam (India) cyberattack(2019)
  - ”Kemurin” water plant attack (2016)
  - Attack on German steel industry(2014)

2. Practical examples

VALUE CHAINS AN ISSUE?

- In the digitalising world, value chains affecting organisations' activities are continuously growing longer and wider
- Number of interdependencies is growing which increases the effects of cyberattacks on different parts of the value chain
- On the field of construction organisation's operations can be affected by attacks on subcontractors, logistic partners, software providers or material production
- Organisation can be unintentional victim of a cyber incident by an attack targeting a subcontractor (Danish railway networks 2022)
- Risk for purposeful influencing through subsidiaries is also growing → supply-chain attack (for example UK's Healthcare 2022)
  - **Attacker carefully searches for a weakest point of a long value chain to gain an effect on better protected targets**
  - Value chain targeting, or through it realising attacks are expected to grow in the future
  - Cross-system integration can make it possible for attacks to spread from one organisation to another
- For protection it is vital to understand which services or products provided by subsidiaries are critical and plan for disturbances on various points of the value chain

2. Practical examples

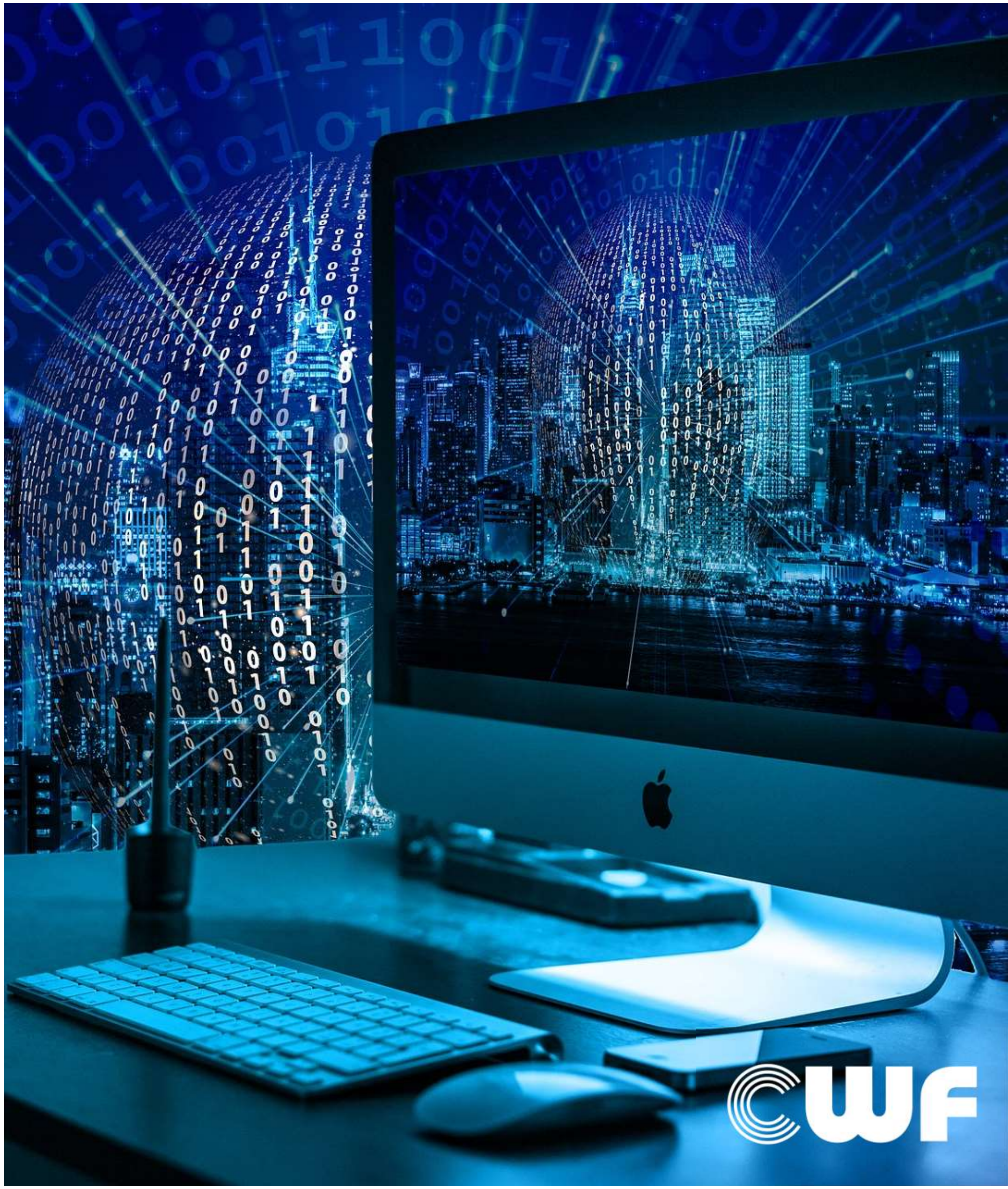
MOST POPULAR ATTACK FORMS

- Ransomware
  - Construction, and real estate field is dependent on projects being delivered on tight deadlines -> lower bar for paying ransom
  - Also increasing amount of critical (valuable) data
- Targeted phishing (spear phishing) or so-called CEO scams
  - Works relatively well on the field as new transactions are common and don't raise suspicion
- Data breaches
- Insider threat
- Attacks on supply chain
  - Dependency on various suppliers, subsidiaries, customers and other partners
  - Criminals often find the weakest link to gain access to other organisations

2. Practical examples

SITUATIONAL PICTURE

- Cyberattacks targeting logistics have doubled during the year of 2022
- Maritime transport and ports as targets have been highlighted, but disturbances have been encountered also on airports and railways
- The vulnerability of transportation and logistics is increased by the same issue plaguing production industries: The number of old OT-systems
- These are for example train control and sensor systems
  - Integrity and availability of data is critical on logistics centres
  - As these systems are not inherently designed to be network controlled, open attack surface and unprotected data is in abundance



MOTIVES

- Cyberattacks targeting the logistics industry highlight not only financial motives, but also those related to disruption and attention.
- Cybercriminals are attracted by the huge amount of customer data available, and the payments demanded for ransomware.
- In the business logic of criminals, the multiplier effects of the logistics industry and the large loss of income caused by even a momentary disruption put pressure on the victim to pay the ransom to the criminal.

CYBERSECURITY IN CONSTRUCTION AND PROPERTY MANAGEMENT AGENDA

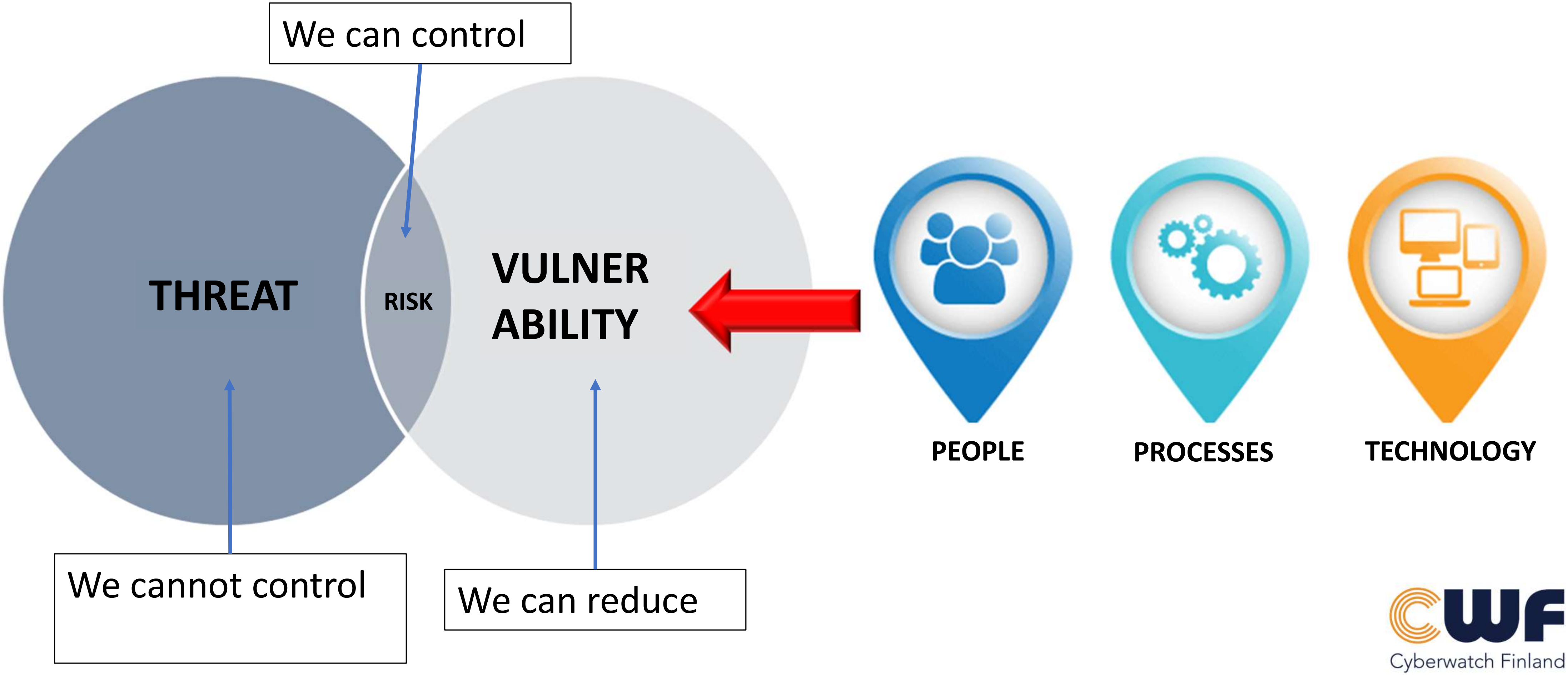
1. Challenges and threats
2. Practical examples
3. ***Improving cybersecurity***

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

Cyberwatch Finland

3. Improving cyber security

THREAT + VULNERABILITY = RISK



We can control

THREAT

RISK

VULNER ABILITY

PEOPLE

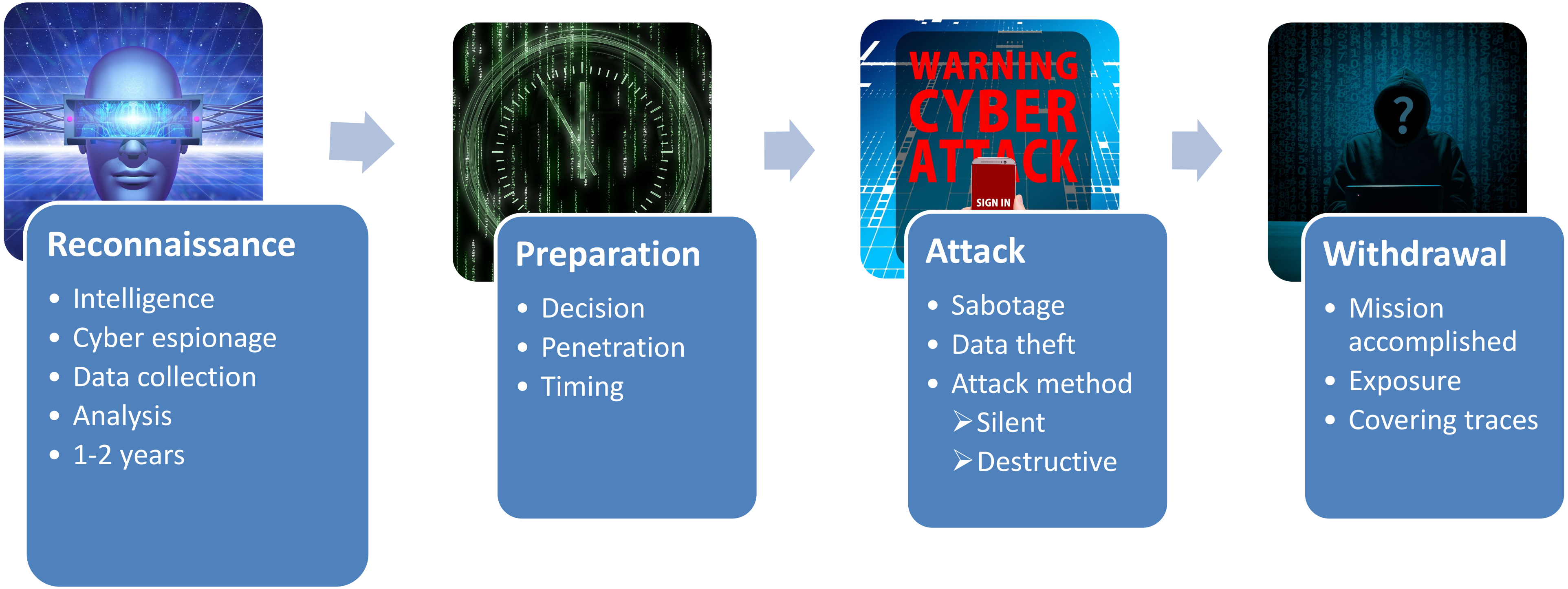
PROCESSES

TECHNOLOGY

We cannot control

We can reduce

STAGES OF A CYBERATTACK



Reconnaissance

- Intelligence
- Cyber espionage
- Data collection
- Analysis
- 1-2 years

Preparation

- Decision
- Penetration
- Timing

Attack

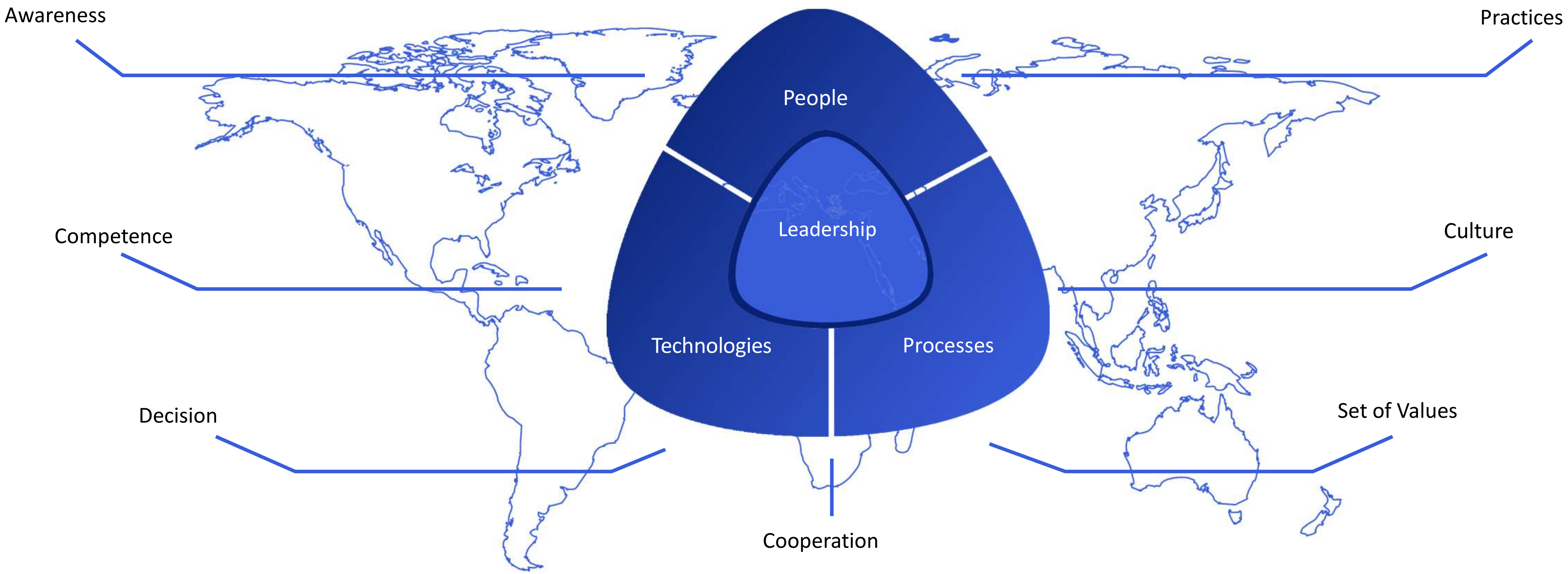
- Sabotage
- Data theft
- Attack method
  - ➢Silent
  - ➢Destructive

Withdrawal

- Mission accomplished
- Exposure
- Covering traces

3. Improving Cybersecurity

WHAT IS CYBERSECURITY



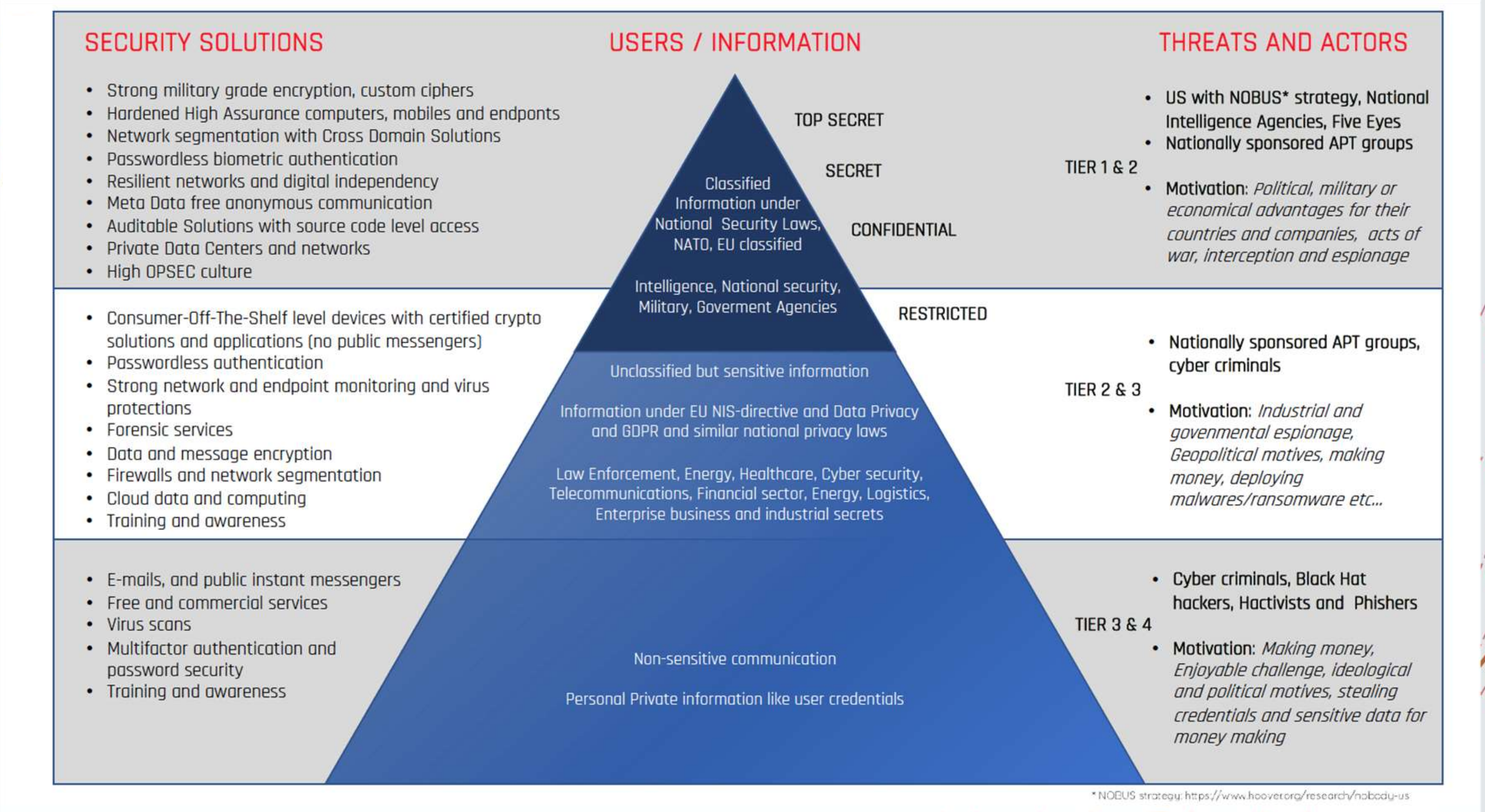
Cyberwatch Finland

Cyberwatch

National cyber security and enterprise cyber security landscape

- We create protection to the highest level for national security needs

- Also we can help to create national cyber security strategy and Center of Excellence which can serve many organisations



SECURITY SOLUTIONS

- Strong military grade encryption, custom ciphers
- Hardened High Assurance computers, mobiles and endponts
- Network segmentation with Cross Domain Solutions
- Passwordless biometric authentication
- Resilient networks and digital independency
- Meta Data free anonymous communication
- Auditable Solutions with source code level access
- Private Data Centers and networks
- High OPSEC culture

- Consumer-Off-The-Shelf level devices with certified crypto solutions and applications (no public messengers)
- Passwordless authentication
- Strong network and endpoint monitoring and virus protections
- Forensic services
- Data and message encryption
- Firewalls and network segmentation
- Cloud data and computing
- Training and awareness

- E-mails, and public instant messengers
- Free and commercial services
- Virus scans
- Multifactor authentication and password security
- Training and awareness

USERS / INFORMATION

TOP SECRET

SECRET

CONFIDENTIAL

RESTRICTED

Classified Information under National Security Laws, NATO, EU classified

Intelligence, National security, Military, Goverment Agencies

Unclassified but sensitive information

Information under EU NIS-directive and Data Privacy and GDPR and similar national privacy laws

Law Enforcement, Energy, Healthcare, Cyber security, Telecommunications, Financial sector, Energy, Logistics, Enterprise business and industrial secrets

Non-sensitive communication

Personal Private information like user credentials

THREATS AND ACTORS

TIER 1 & 2

- US with NOBUS* strategy, National Intelligence Agencies, Five Eyes
- Nationally sponsored APT groups
- Motivation: *Political, military or economical advantages for their countries and companies, acts of war, interception and espionage*

TIER 2 & 3

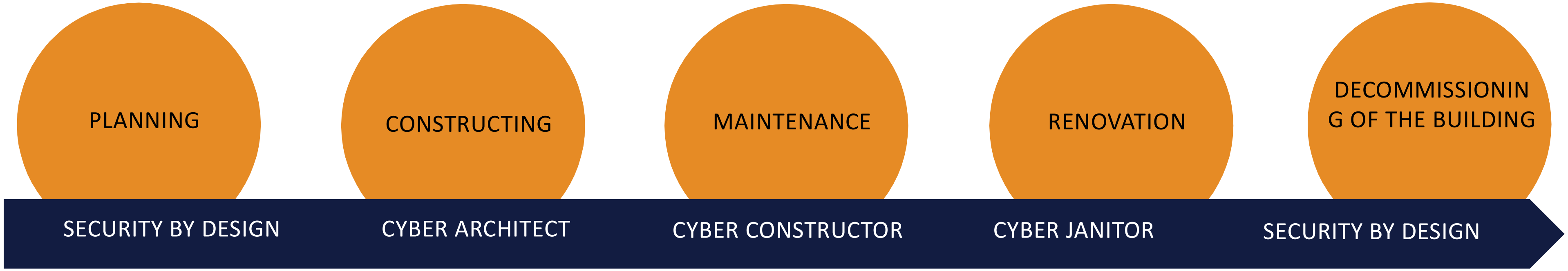
- Nationally sponsored APT groups, cyber criminals
- Motivation: *Industrial and govenmental espionage, Geopolitical motives, making money, deploying malwares/ransomware etc...*

TIER 3 & 4

- Cyber criminals, Black Hat hackers, Hactivists and Phishers
- Motivation: *Making money, Enjoyable challenge, ideological and political motives, stealing credentials and sensitive data for money making*

* NOBUS strategy: https://www.hoover.org/research/nobody-us

CYBERSECURITY INCLUDED THROUGHOUT THE BUILDING'S LIFE CYCLE



PLANNING

CONSTRUCTING

MAINTENANCE

RENOVATION

DECOMMISSIONIN G OF THE BUILDING

SECURITY BY DESIGN

CYBER ARCHITECT

CYBER CONSTRUCTOR

CYBER JANITOR

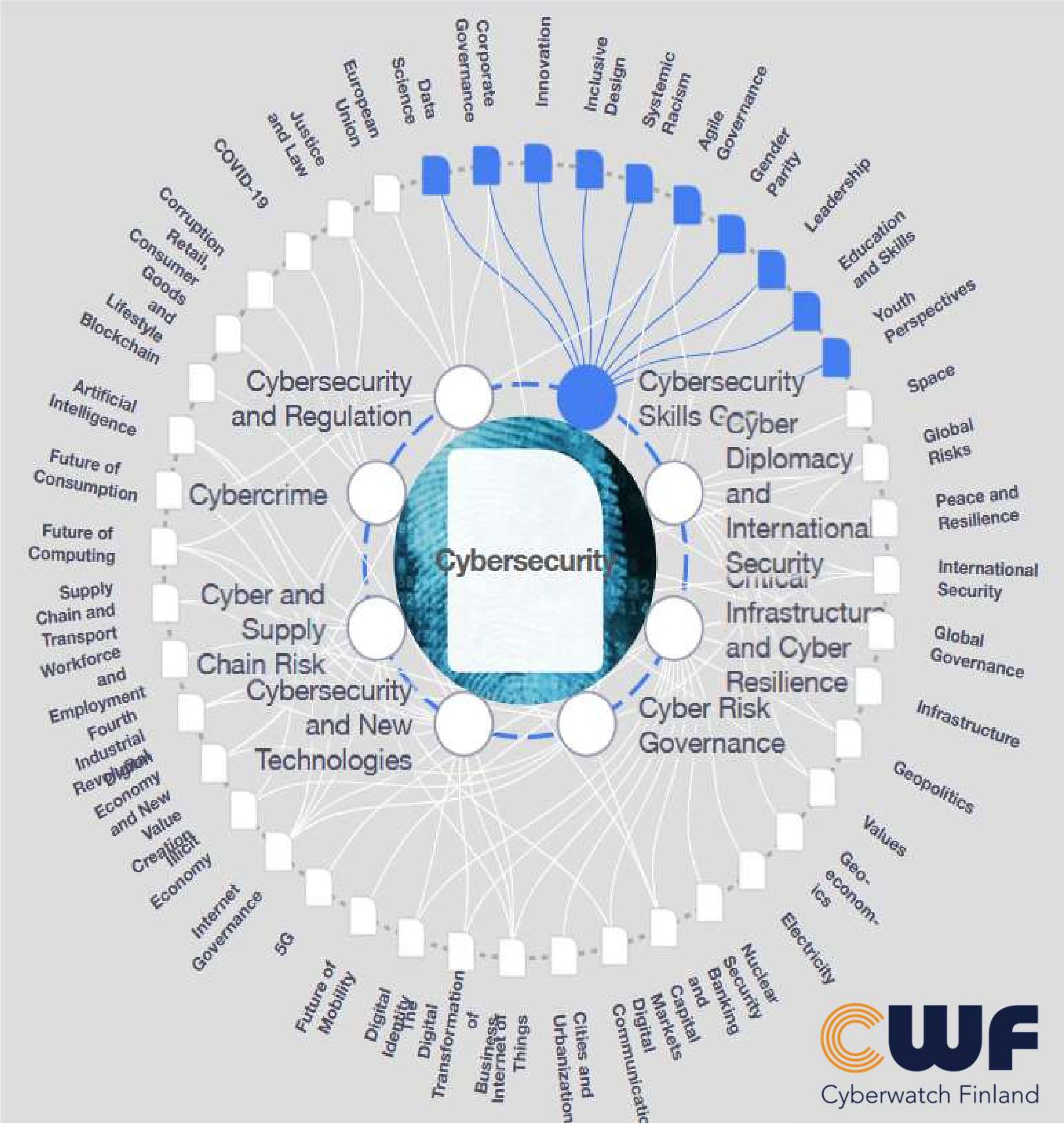
SECURITY BY DESIGN

Cyberwatch Finland

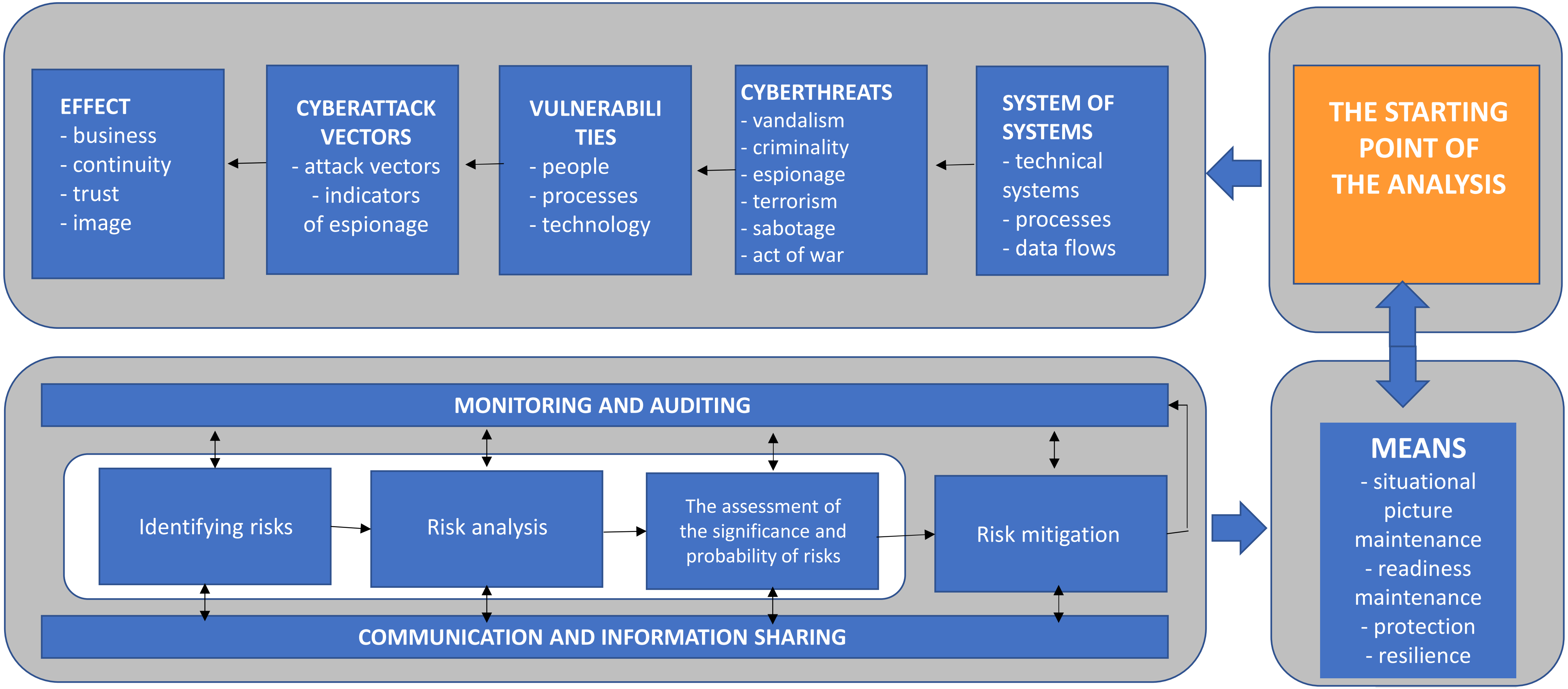
3. Improving Cybersecurity

CYBER MANAGEMENT – A WINNING CONCEPT ”TAKE THE CONTROL BACK”

- ➢ Comprehensive and reliable cyber situational picture for top management
- ➢ Reliable and credible cyber risk analysis and risk management system
- ➢ An agile cyber preparedness and continuity management plan
- ➢ A well-trained and practiced crisis management organisation
- ➢ Appropriate cyber training for all personnel
- ➢ The right and innovative cyber technology choices
- ➢ A correctly measured cyber budget
- ➢ A flexible and ever-evolving cyber culture



CYBER THREAT ANALYSIS



EFFECT
- business
- continuity
- trust
- image

CYBERATTACK VECTORS
- attack vectors
- indicators of espionage

VULNERABILITIES
- people
- processes
- technology

CYBERTHREATS
- vandalism
- criminality
- espionage
- terrorism
- sabotage
- act of war

SYSTEM OF SYSTEMS
- technical systems
- processes
- data flows

THE STARTING POINT OF THE ANALYSIS

MONITORING AND AUDITING

Identifying risks

Risk analysis

The assessment of the significance and probability of risks

Risk mitigation

COMMUNICATION AND INFORMATION SHARING

MEANS
- situational picture maintenance
- readiness maintenance
- protection
- resilience

CYBER RISK MANAGEMENT PROCESS

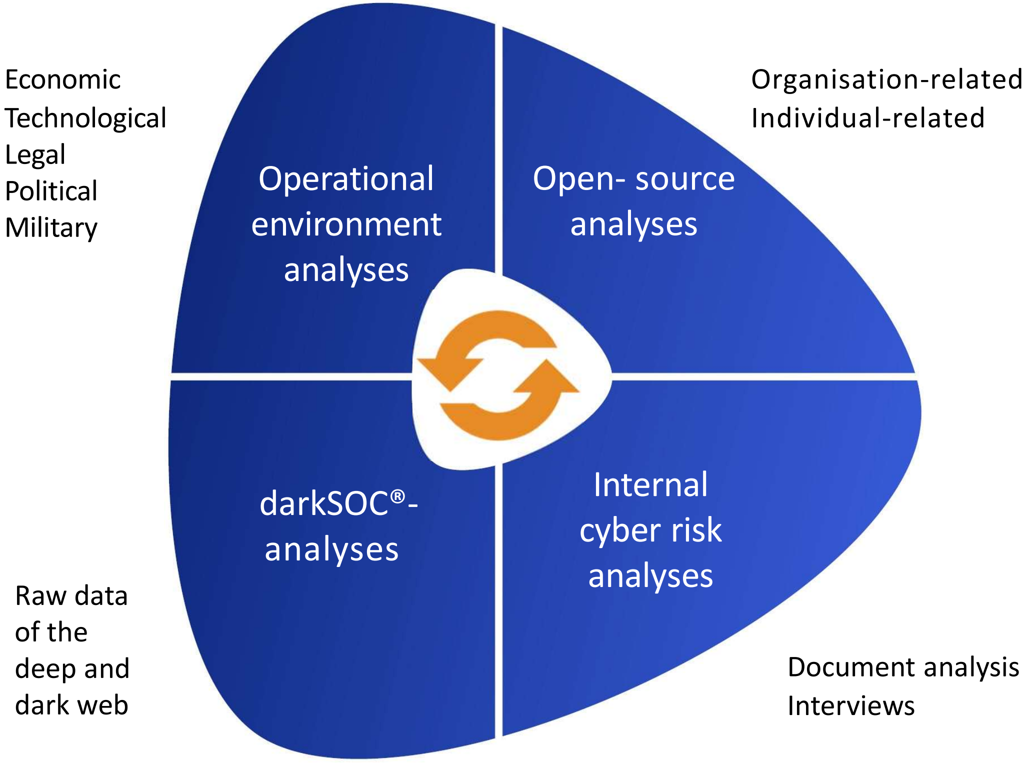
Cyberwatch Finland

3. Improving Cybersecurity

A COMPREHENSIVE CYBER SITUATIONAL PICTURE

A comprehensive cyber situational picture is formed with the help of the modular services developed by Cyberwatch Finland, where the necessary data is collected in numerous different ways.

For DarkSOC® – analysis, raw data is collected on servers at 9 Gb/s non-stop. The data can be used to analyse the organisation's exposures, reveal leaks and other potential problem areas, and analyse the risks caused by these to the business.



Economic
Technological
Legal
Political
Military

Operational environment analyses

Open- source analyses

Organisation-related
Individual-related

darkSOC®- analyses

Internal cyber risk analyses

Raw data
of the
deep and
dark web

Document analysis
Interviews

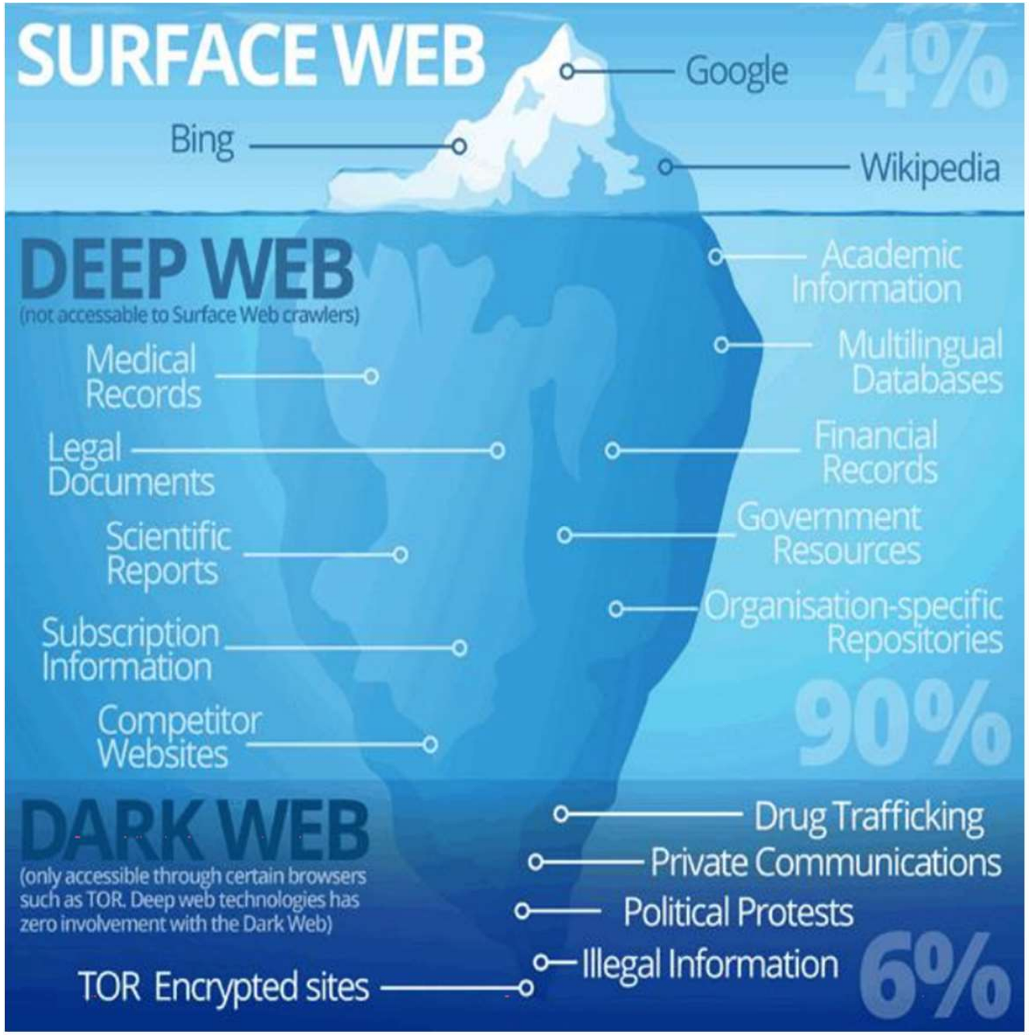
Cyberwatch Finland

CYBERWATCH SPECIAL TOOLS

CWF
Analytics

darkSOC®
Analysis

darkSOC®
Anlysis

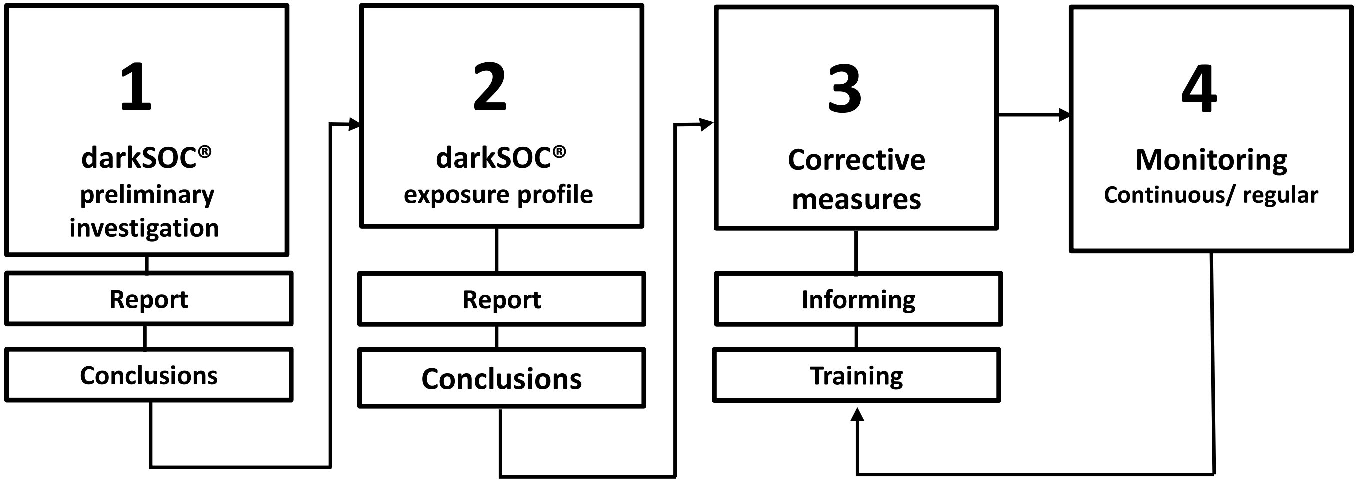


Cyberwatch Finland

DarkSOC® -PLAYBOOK

With darkSOC® analysis, we find out your organisation's profile and level of exposure in the dark and deep web. Data is collected non-stop at 9 Gb per second on servers located around the world. The analysis reveals your organisation's cybersecurity gaps, leaked data and other potential problem areas. With the help of analysis, you get a view of how the organisation looks from the eyes of a cybercriminal. We classify the effects of cyber exposure into eight categories.

We have described below the steps of the darkSOC process, which can help to reduce malicious visibility on the dark web, increase resilience and improve overall cybersecurity.

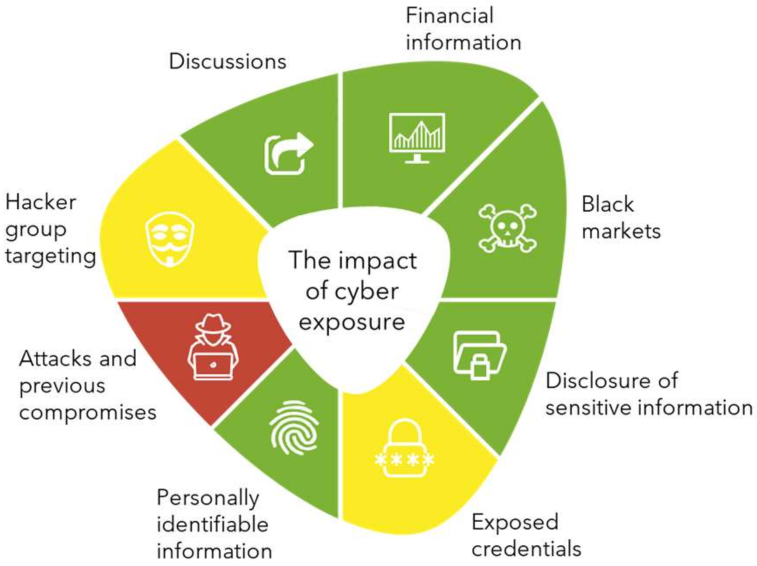


1
darkSOC®
preliminary investigation
Report
Conclusions

2
darkSOC®
exposure profile
Report
Conclusions

3
Corrective measures
Informing
Training

4
Monitoring
Continuous/ regular



The impact of cyber exposure

Financial information

Black markets

Disclosure of sensitive information

Exposed credentials

Personally identifiable information

Attacks and previous compromises

Hacker group targeting

Discussions

CWF
Cyberwatch Finland

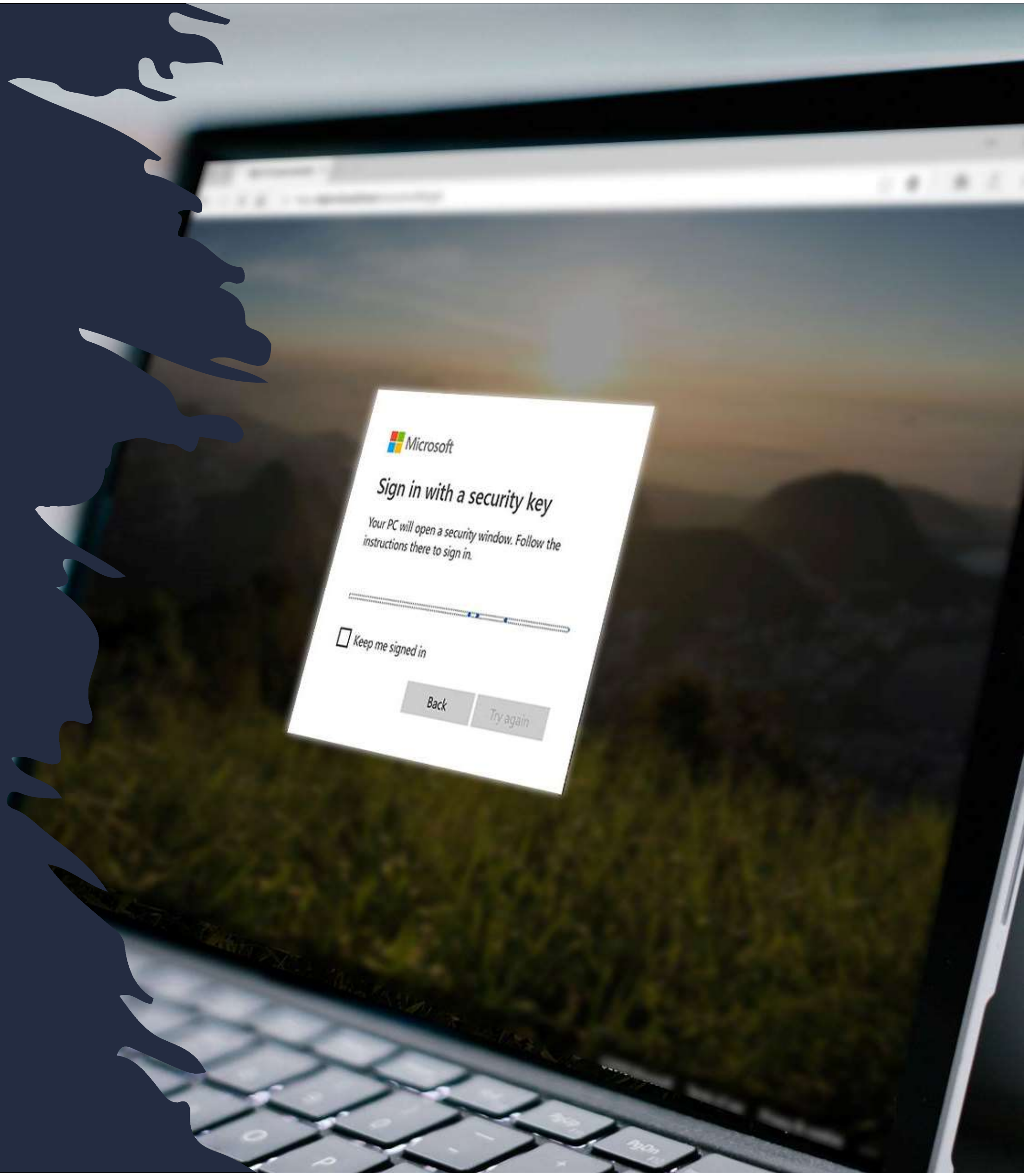
The password problem

81% of successful cyber attacks are due to stolen or lost password

(Source: Verizon Data Breach Investigation 2020)

Cyberwatch

Passwordless Authentication stops 99.9% of all cyberattacks against digital identities



Sign in with a security key

Your PC will open a security window. Follow the instructions there to sign in.

Cyberwatch

THANK YOU

aapo@cyberwatchfinland.fi

CWF

Cyberwatch Finland