

CYBERWATCH FINLAND

The cyber security situation in Finland during the Ukrainian war and what kind of intelligence is needed.

Pertti Jalasvirta



Pertti Jalasvirta, Partner/Founder Cyberwatch Oy

EXPERIENCE:

Management team and board level in Finland and international

Development and International training (AETHER)

CBRN protection and safety, international training activities

Development of field hospitals and safety

International speaker

Strategic cybersecurity

Associate Fellow,

Geneve Centre For Security Policy, GCSP

EDUCATION:

Degrees in management (Cybermaster), product development, entrepreneurship and media management

Dark and Deep web analysis and intelligence research

Research and development of social physics

Publications:

Knowledge mining of unstructured information, Implementing

RFID technology in a novel triage system during a simulated mass casualty situation.

Articles:

Project Aether – Air Passenger Transport Security in Case of CBRN Terrorism

CONTENT OF THE PRESENTATION

1. Background to the strategic cybersecurity situational awareness
2. The state of cyber security in Finland in 2022
3. Cyber intelligence (Centre of excellence)
4. Competence development
5. Foresight
6. Q&A

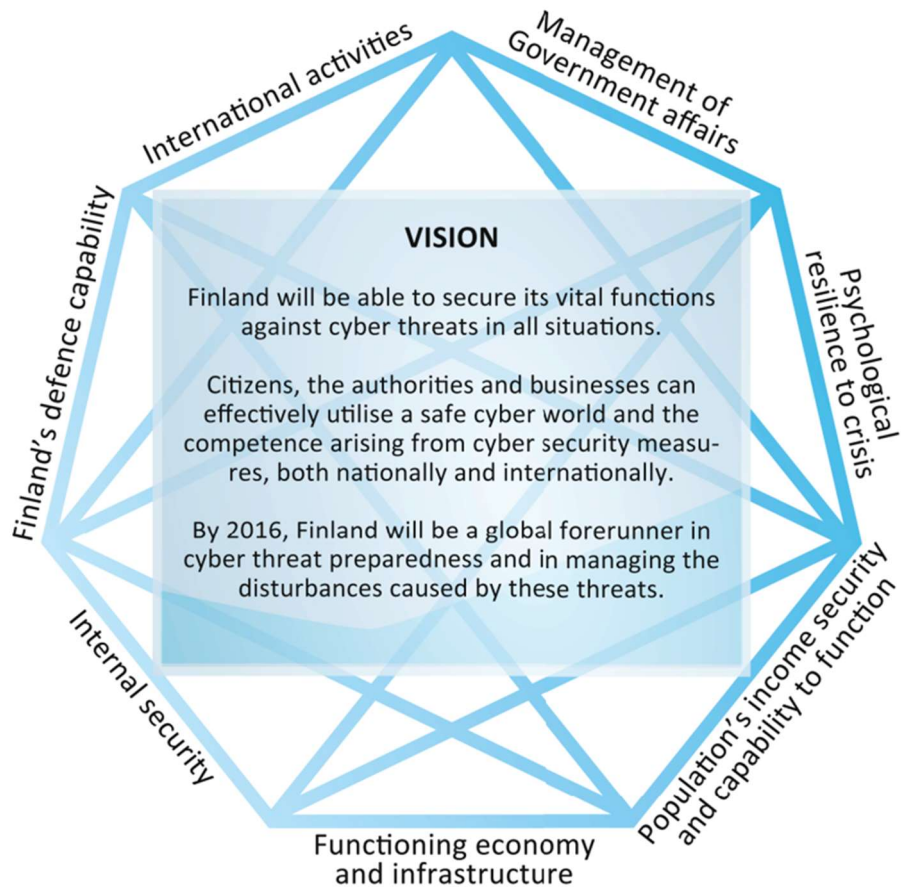
THE BACKBONE OF CYBER SECURITY IS LEADERSHIP



CYBER SECURITY LEADERSHIP

- **Comprehensive and reliable Cyber Security Awareness**
- **Adequate capacity for Cyber Risk Assessment and management**
- **Agile Cyber preparedness and continuity plan**
- **Well-trained Cyber crisis management competence**
- **Superiority Cyber competence at the human sector**
- **Superiority Cyber technologies – smart choices**
- **Adequate Cyber budget**
- **Agile and Comprehensive Cyber culture**

THE STATE OF CYBER SECURITY IN FINLAND IN 2022



Finland's relative position as a good cyber security country has weakened since 2012.

Various international indices measure the cyber security capabilities of countries, and in these assessments our country's position in relation to others has decreased, although we have developed our own actions.

GLOBAL CYBER SECURITY INDEX

Finland
- Index 0.618
- EUR: 5
- Global: 8



GCI 2017

Finland
- Index 0.741
- EUR: 6
- Global: 16

GCI 2014

GCI 2018

Finland
- Index 0.856
- EUR: 10
- Global: 19

GCI five pillars – (1) Legal Measures, (2) Technical Measures, (3) Organizational Measures, (4) Capacity Development, and (5) Cooperation.

GCI 2020

Finland
- Index 0.958
- EUR: 14
- Global: 22

NATIONAL CYBER SECURITY INDEX

<https://www.security-risks.com/post/national-cyber-security-index-2022>

- Finland
- Index 79,22
 - Rank: 6
 - DDL: 82,26
 - Dif: -3,04

NCSI
2018



NCSI 2020

- Finland
- Index 85,71
 - Rank: 10
 - DDL: 79,48
 - Dif: +6,23

EVERYTHING IS BASED ON KNOWLEDGE

The statement of the Parliamentary Committee on the Future states:

"After all, the issue of cybersecurity is not technological, but the best way to protect against threats is to increase citizens' knowledge and understanding of digitalization and critical media literacy."



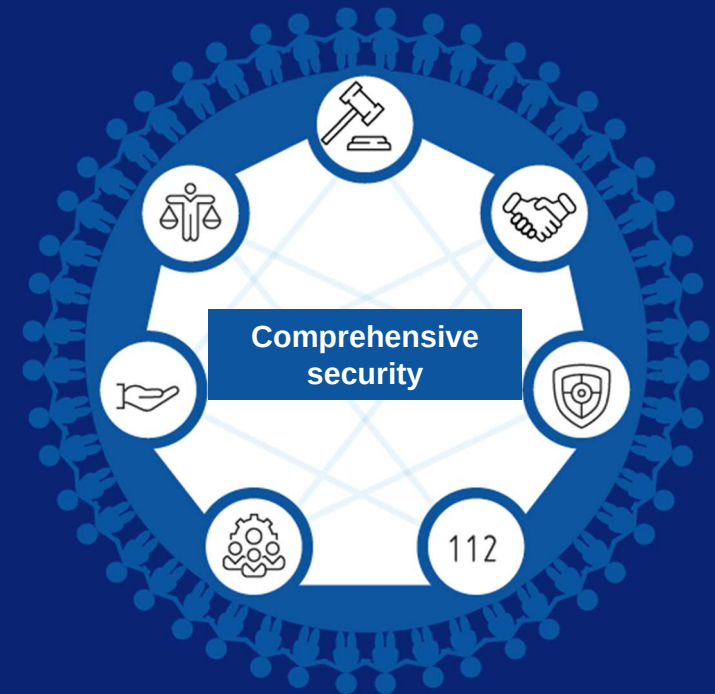
COMPREHENSIVE SECURITY

What is comprehensive security?

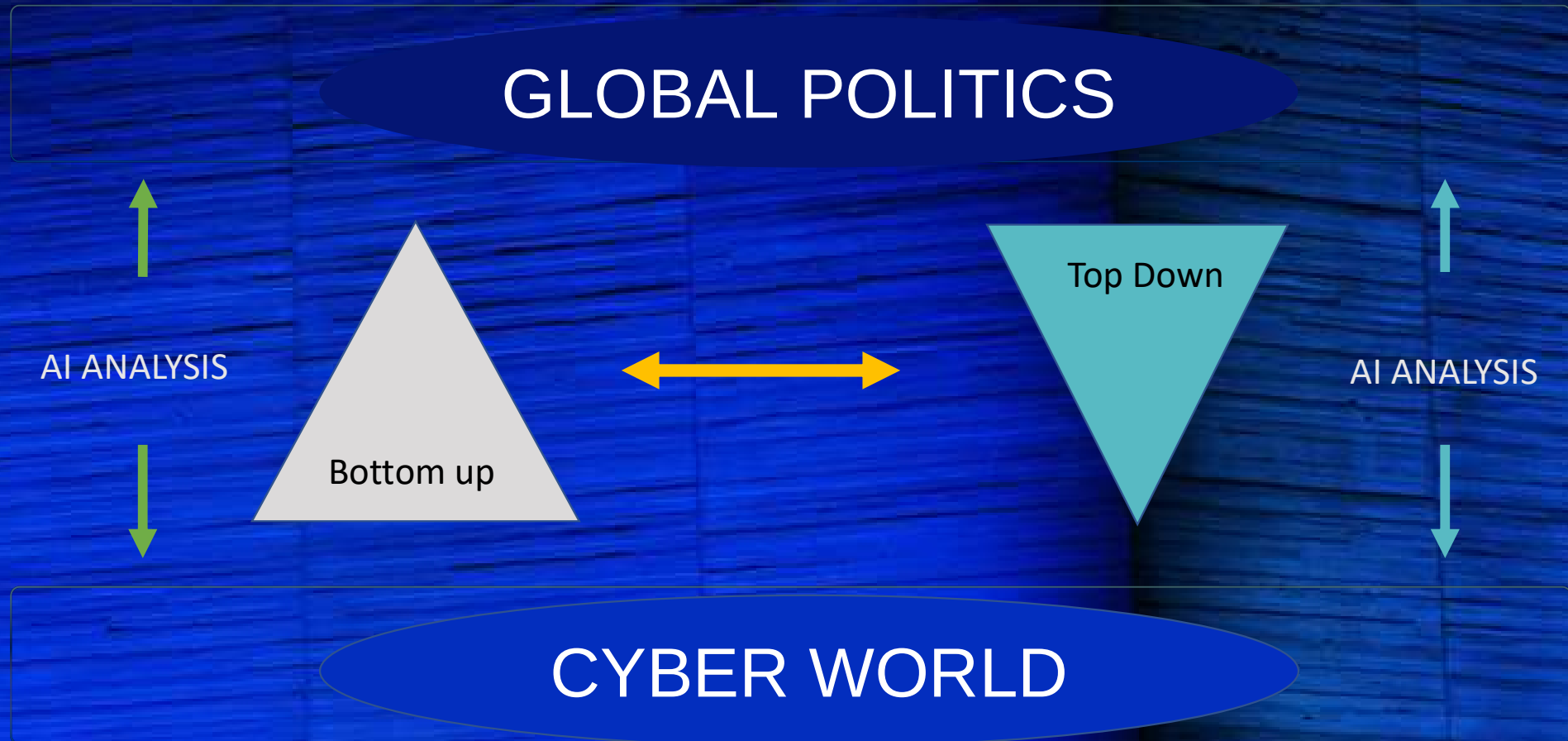
Comprehensive security is the cooperation model of Finnish preparedness, where vital societal functions are handled together by authorities, businesses, NGOs and citizens.

Vital societal functions are:

- Leadership
- International and EU activities
- Defense capability
- Internal security
- Economy, infrastructure and security of supply
- Functional capacity of the population and services
- Psychological resilience



STRATEGIC CYBER ANALYSIS



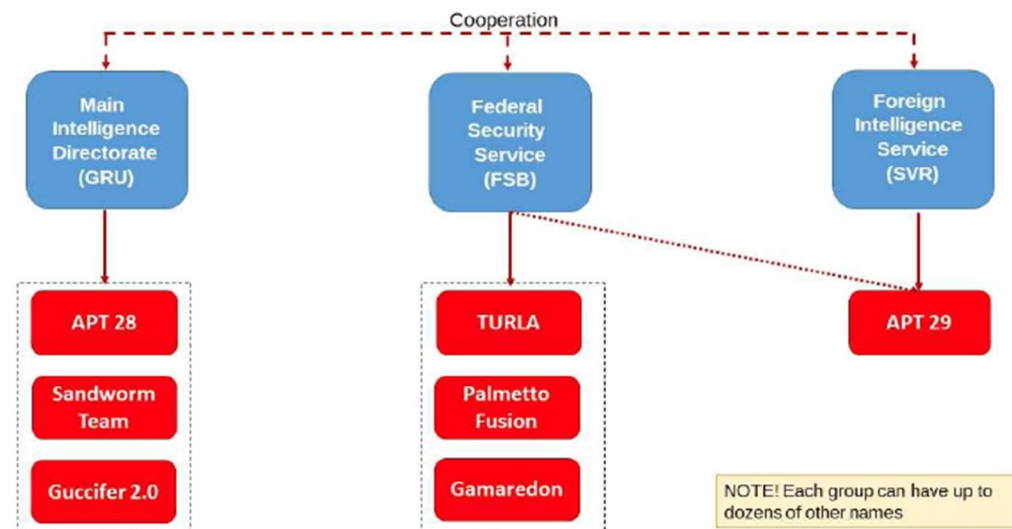


8 MINUTE READ

RUSSIA'S BACKGROUND IN CYBER WARFARE

Special reports for the preparation of cyber situational awareness

The most significant hacker groups in Russia

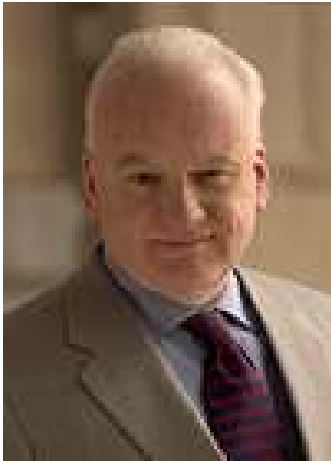


Sources: Cunningham, Conor. *A Russian Federation Information Warfare Primer*, Research report, University of Washington, 12.11.2020
Russian Cyber Units, Congressional Research Service, January 4, 2021

CYBERWARFARE

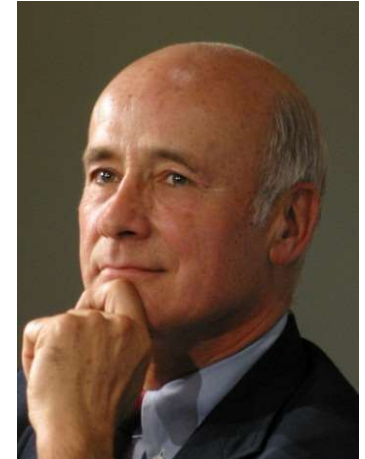
“Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption”

Richard A. Clarke, 2010



“Cyber war is hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.”

Joseph S. Nye Jr. 2011



“Refers to the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems.”

Myriam Dunn Cavelty, 2010



RUSSIA'S CYBER WARFARE CONCEPT

Voiman Venäjä

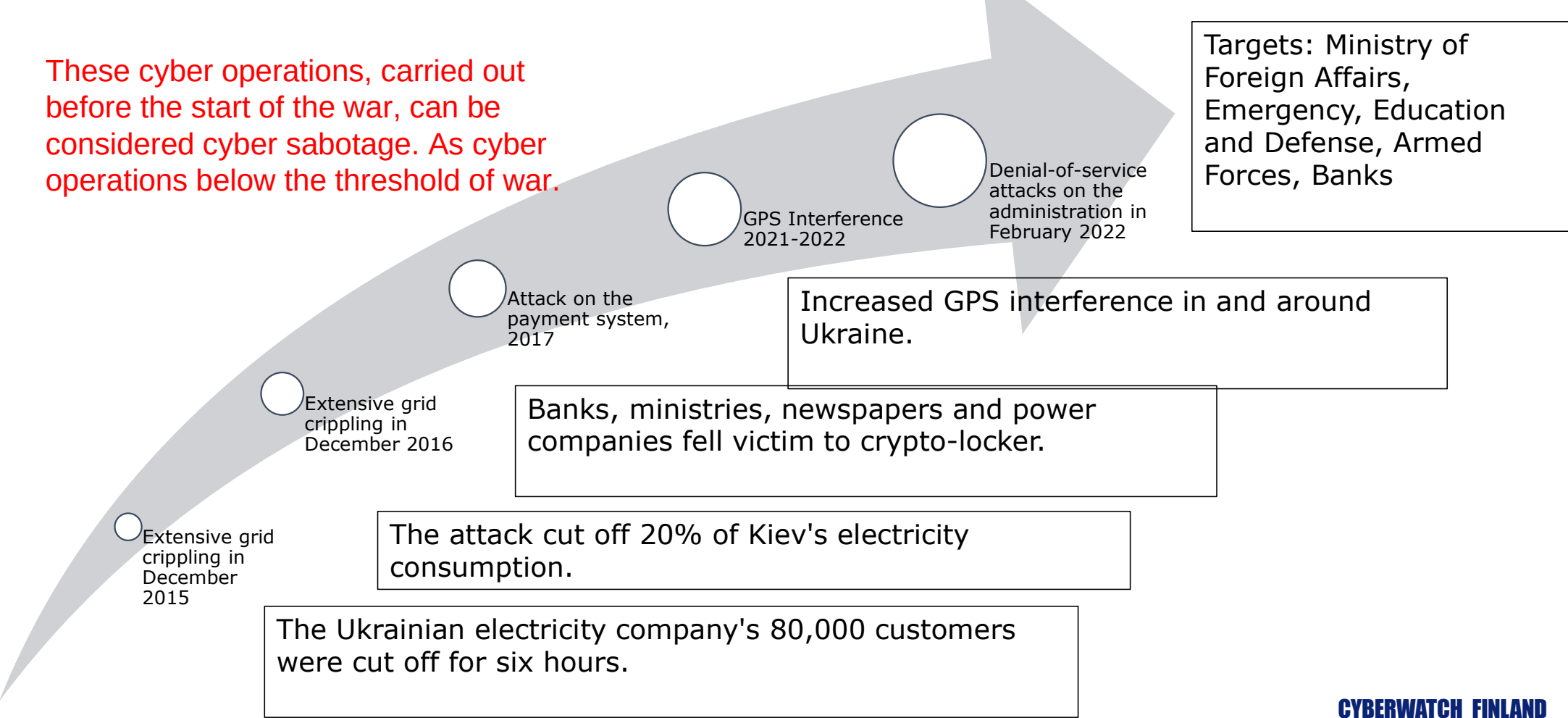


Lähde: PLM, Voiman Venäjä, tutkimusraportti, 2019

- Russian information warfare includes attacks on information networks, electronic warfare and information psychological influence.
- At the beginning of the military conflict, Russia's cyber capabilities are likely to be used to disrupt the adversary's mobilization and troop transfers, to weaken situational awareness, to paralyze leadership capabilities and, as part of long-term influencing, to support the actual military action.
- Cyber capabilities are a tool for Russians to carry out larger information operations in which the target is the situational understanding, operational capability and will of a potential adversary.
- For the Russians, cyber capabilities are part of the wide range of means of the strategic disincentive and therefore it is not appropriate to organize them purely militarily.

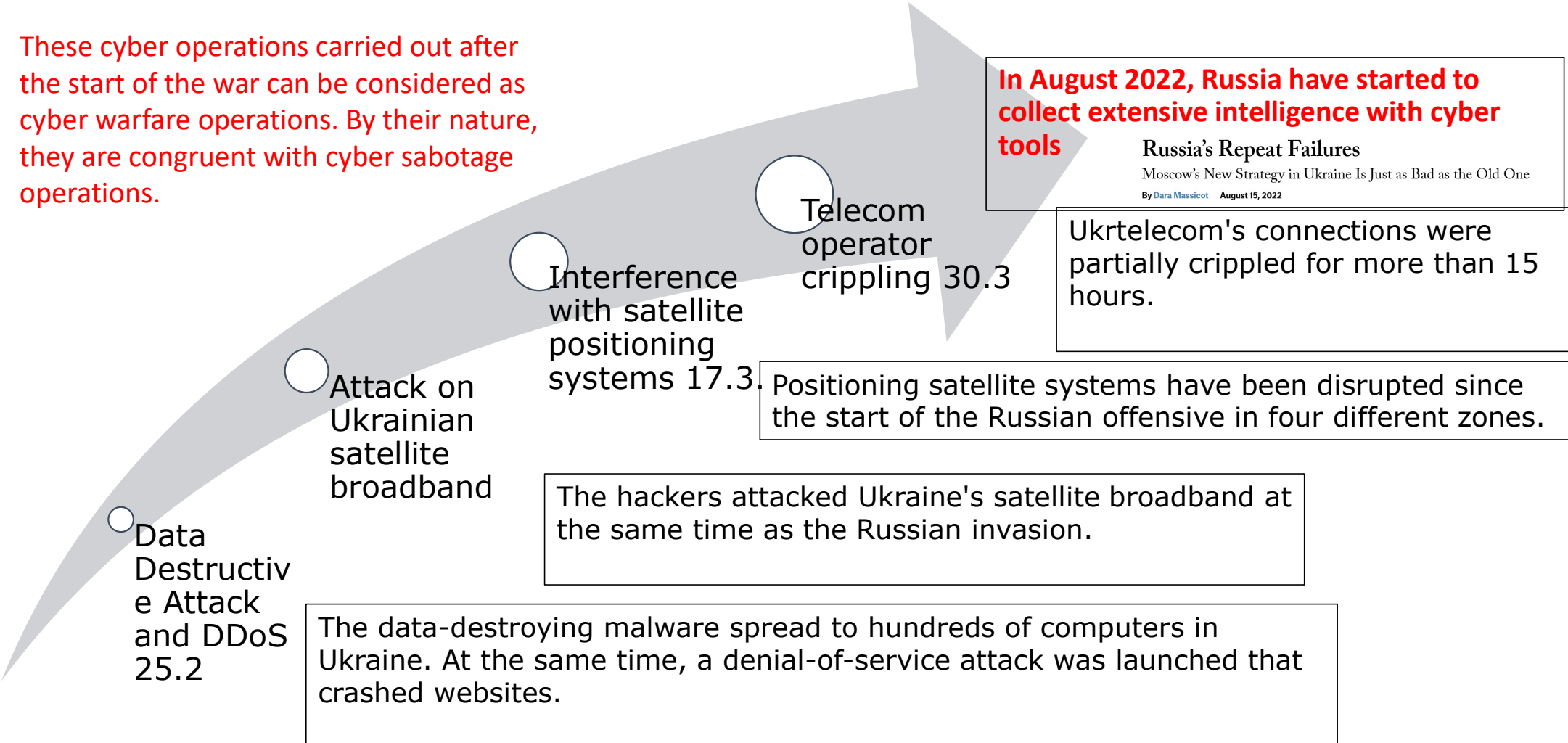
CYBER OPERATIONS IN UKRAINE BEFORE 24/02/2022

These cyber operations, carried out before the start of the war, can be considered cyber sabotage. As cyber operations below the threshold of war.



CYBER OPERATIONS IN UKRAINE AFTER 24/02/2022

These cyber operations carried out after the start of the war can be considered as cyber warfare operations. By their nature, they are congruent with cyber sabotage operations.



WEAK EFFECTIVENESS OF RUSSIA'S ACTIVITIES

Possible reasons for a poor result:

- The proxies used by Russia may not have been top experts in this type of attack
- Coordination and management of cyberattacks poorly implemented
- With the help of the West, already in the fall of 2021, Ukraine's critical infrastructure could be "cleaned" of possible backdoors and kill switches
- Russia has not wanted to use all the attacking capabilities – something left in their back pocket for future actions
- Russia has not wanted to use all cyber attack capabilities. Advanced cyber weapons can only be used once = advanced countermeasures?

TARGETS OF CYBERATTACKS AT DIFFERENT STAGES (WHAT)

Goals months/years before the armed attack:

Malware testing
Testing cyberattack vectors
Reconnaissance and targeting of the operating environment,
Installation of rear gates and kill switches,
Producing uncertainty and mistrust.

Goals just before the armed attack:

Crippling critical systems,
Manipulation and destruction of data,
Intelligence of the operating environment,
Distorting the situational picture,
Creating uncertainty and mistrust: "Your administration is incapable of taking care of you"

**Cyber-sabotage
operations against
critical infrastructure**

**Cyberwarfare operations against
critical infrastructure**

Goals during the attack:

Crippling/destroying military capabilities,
Management of critical information infrastructure,
Operating environment intelligence,
Producing uncertainty, mistrust and chaos.

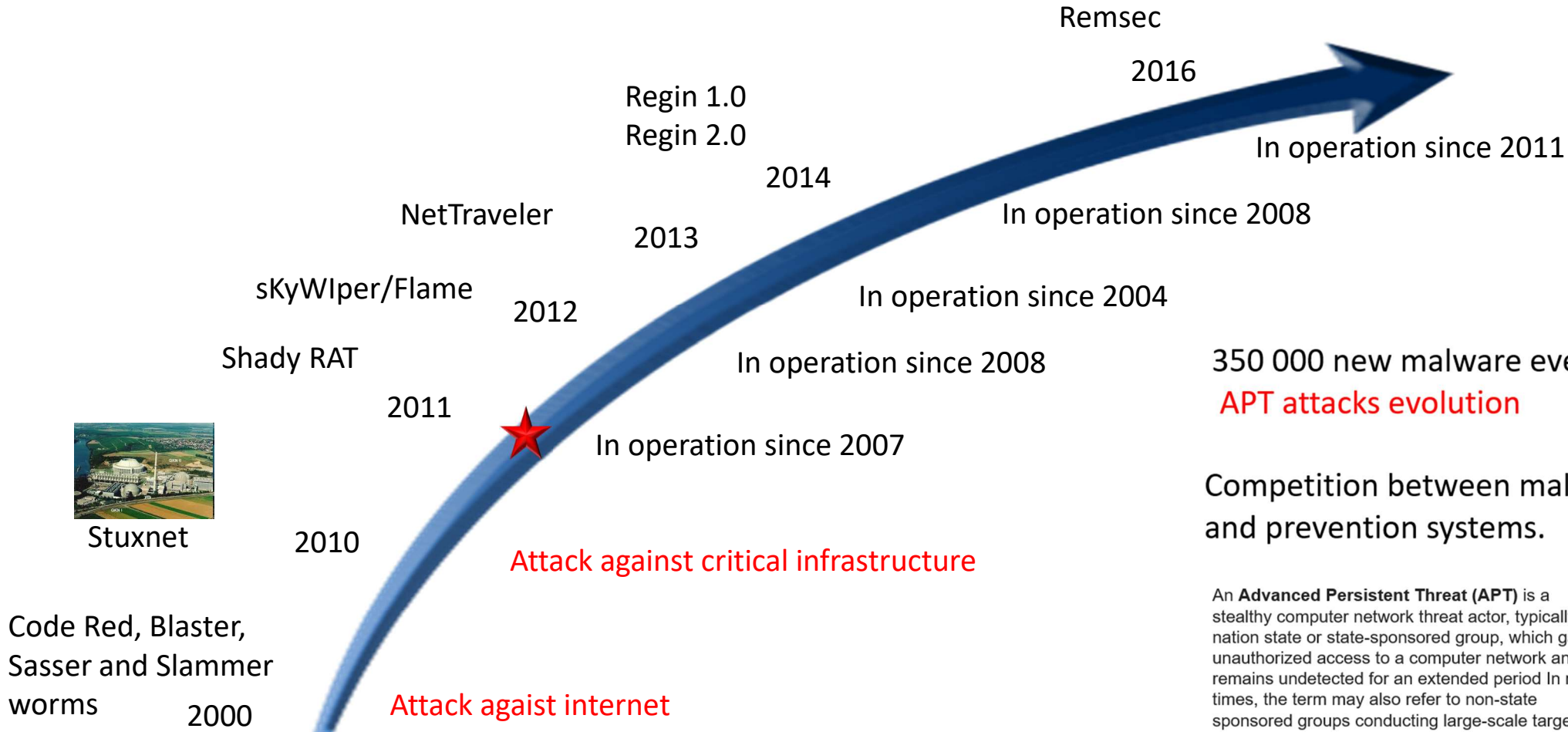
CYBERSPACE OPERATION – MOTIVATION?

-  Cyber warfare
-  Cyber sabotage
-  Cyber terrorism
-  Cyber espionage
-  Cyber-crime
-  Cyber vandalism

- Attack to paralyze the function vital to society*
- Attack to disrupt the function vital to society*
- Attack to create chaos in society*
- Attack to hide actual cyber espionage attack*
- Attack to get money (ransoms)*
- Attack to harm the organization*

DDOS-attack motivation

APT ATTACKS EVOLUTION



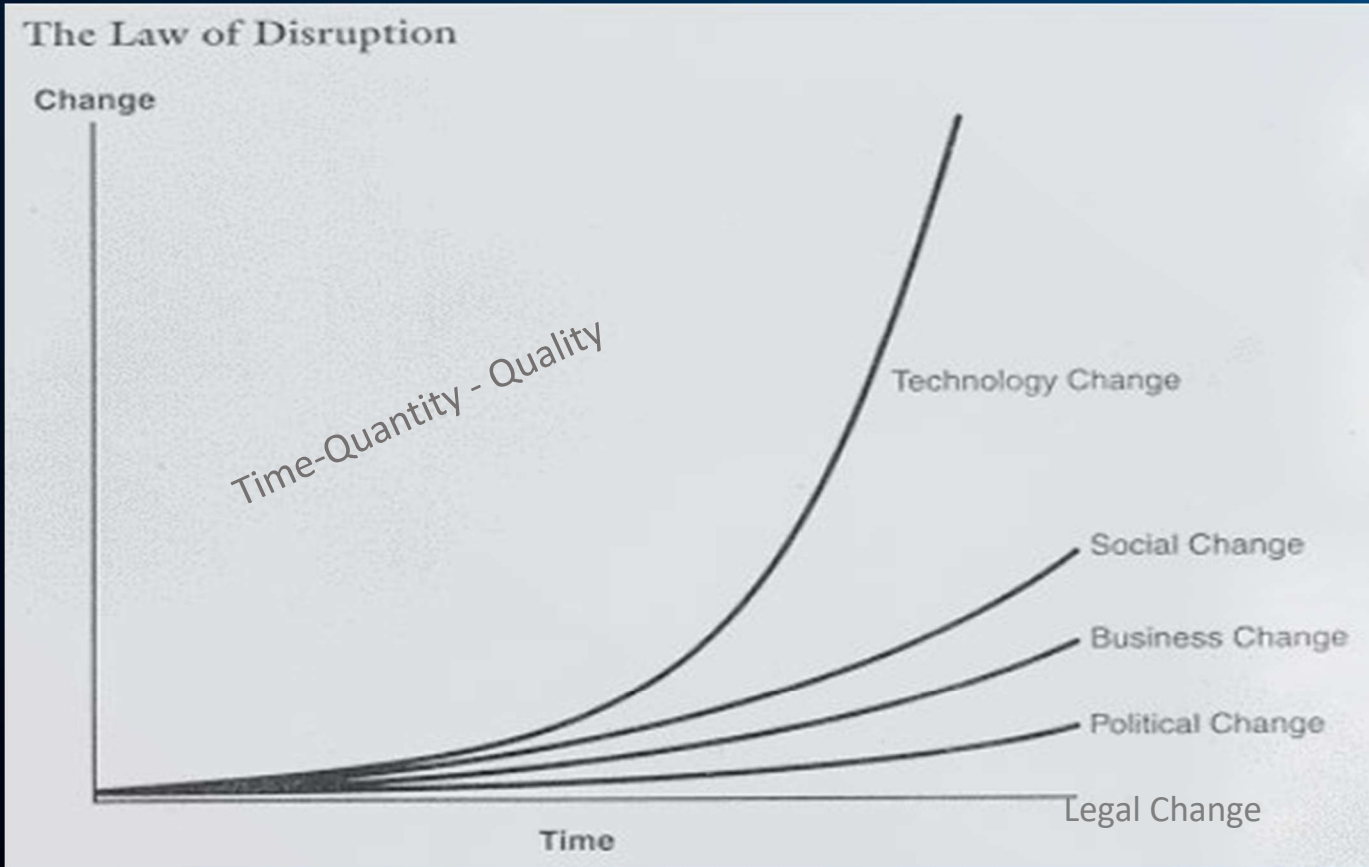
Stuxnet

350 000 new malware every day.
APT attacks evolution

Competition between malwares and prevention systems.

An **Advanced Persistent Threat (APT)** is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state sponsored groups conducting large-scale targeted intrusions for specific goals.

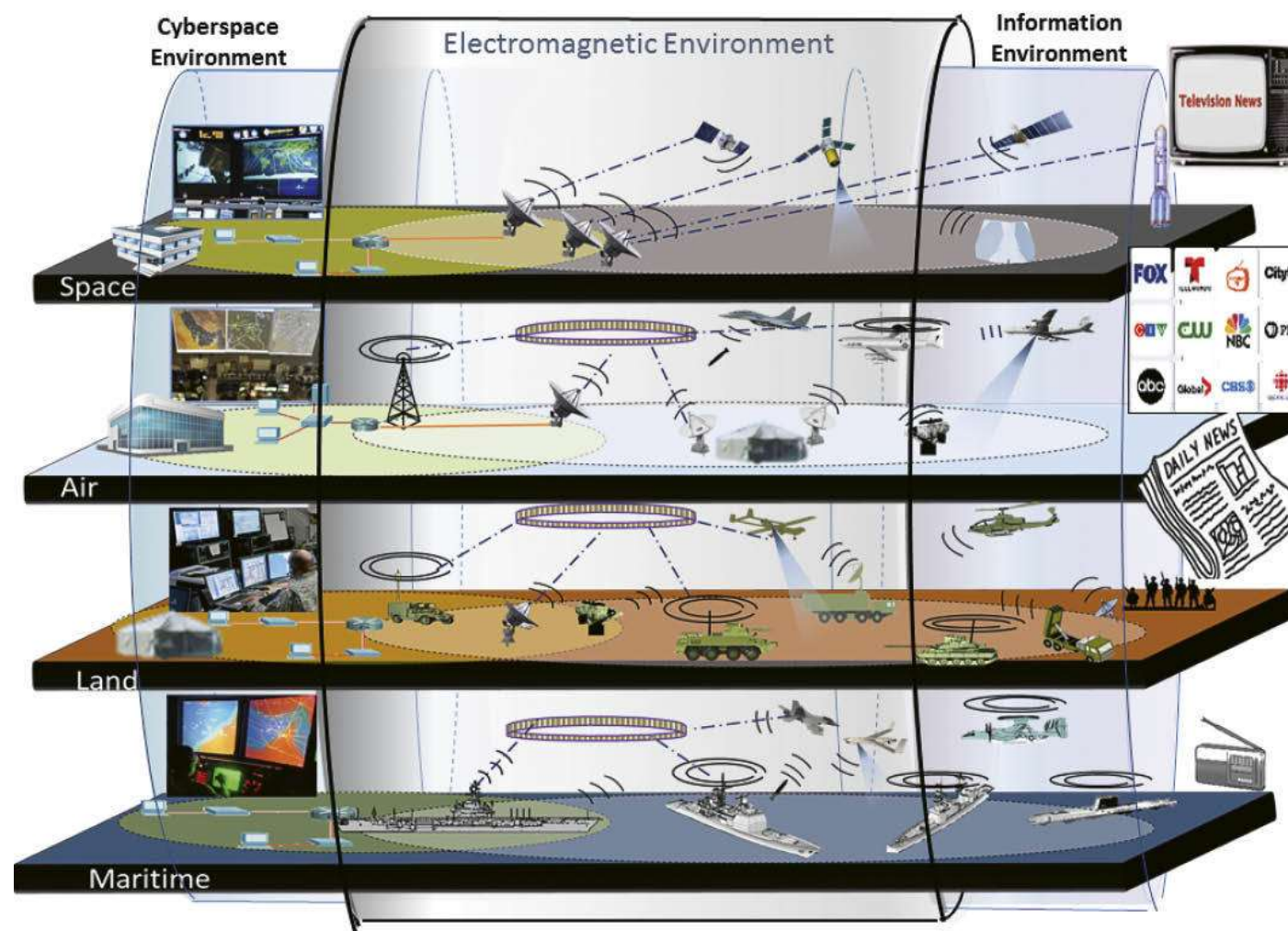
DYTOPIA: FROM HISTORY TO THE FUTURE (WHY)



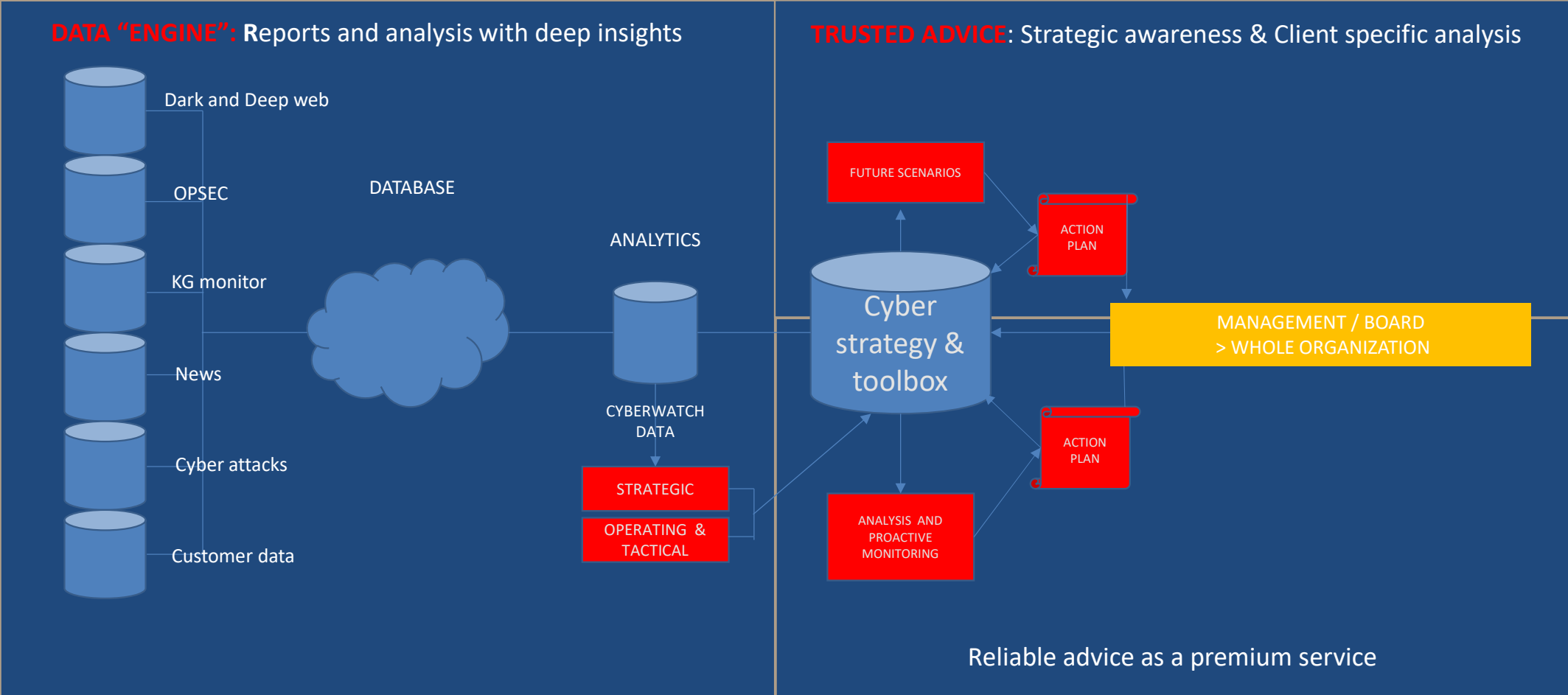
DIGITAL ENVIRONMENT (WHERE)

Cyber, the electromagnetic spectrum and the information environment form a new digital and interdependent operating environment.

Disruptions and attack operations affect these environments because they are closely interconnected with each other.



CYBERWATCH CYBER INTELLIGENCE – STRATEGIC – OPERATING – TACTICAL LEVELS



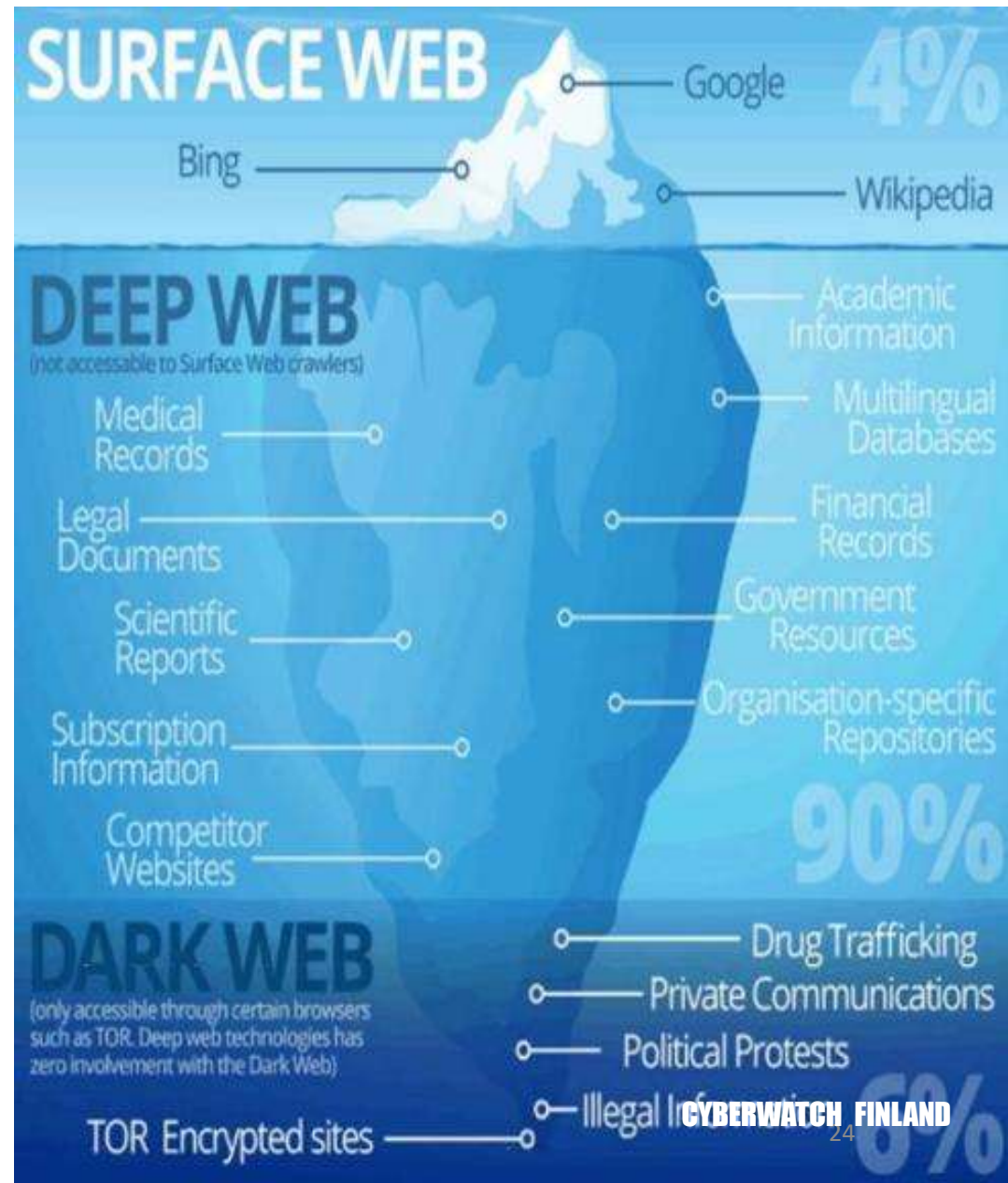
WHAT ARE DARK WEB AND DEEP WEB?

THE UN-INDEXED PART OF INTERNET

Publicly available search engines like Google cover only a certain portion of the internet. This is the visible part that we call the surface web. However, where the surface web ends, the deep web begins. The deep web is everything you can access with your browser that is not indexed by search engines. This could be your e-mail accounts, intranet, data leakage platforms, some discussion forums, private blogs, etc.

THE DARK WEB AND TECHNICAL ANONYMITY

The dark web refers to a technology that makes surfing sessions more private – technically anonymous. These technologies include TOR and I2P. For instance, in TOR, there are 7 layers of encryption before the packet reaches the desired host. This is why nobody knows who is surfing and where the servers are.



WHAT IS CYBER SECURITY EXPOSURE?

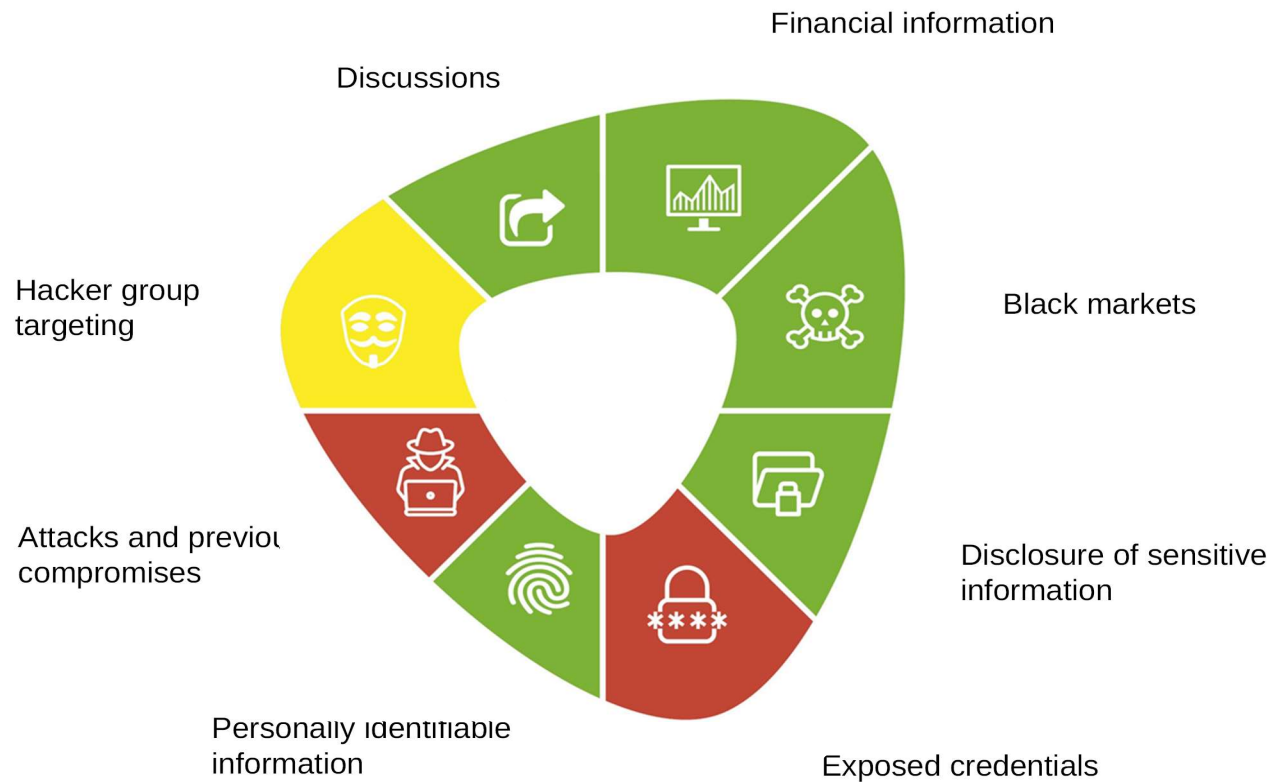
Cyber Security Exposure is the measure of harmful cyber visibility in Dark and Deep Web

The visibility depends on many things e.g., number of on-line ICT assets, level of organization's integration with others, amount of shared information.

Moreover, an exposure can come in many forms like technical vulnerabilities, personal information, source codes, internal emails etc.



All data lost to the Dark Web, even if only lost once, will remain there forever and be refined with new attacks



DARKSOC® - SERVICE CONCEPT

The **DARKSOC®** service collects and utilises information in various ways:

- Deep and Dark web data are collected on Cyber Intelligence House's global servers 24/7 and 9 Gb per second.
- The data can be used to analyze the cyber exposure of the organisation, to reveal leaks and other potential problem areas.
- Information from several open sources complements the profile of the organisation and related persons.
- The analysis of the operating environment provides a view of events, trends and phenomena affecting the organisation from different perspectives.
- The organisation's internal cyber risk analysis including interviews and documentation review provides an overall picture of internal risk factors.



Lost data is sold on Dark and Deep online marketplaces and at a reasonable price

Social Media	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Hacked Facebook account	\$75	\$65	-\$10
Hacked Instagram account	\$55	\$45	-\$10
Hacked Twitter account	\$49	\$35	-\$14
Hacked Gmail account	\$156	\$80	-\$76
Instagram followers x 1000	\$7	\$5	-\$2
Spotify followers x 1000	\$3	\$2	-\$1
Twitch followers x 1000	\$6	\$5	-\$1
LinkedIn x 1000	\$10	\$12	+\$2
Pinterest followers x 1000	\$5	\$4	-\$1
Soundcloud plays x 1000	\$1	\$1	\$0
Twitter retweets x 1000	\$25	\$25	\$0
Instagram likes x 1000	\$6	\$5	-\$1

France Passport	\$4,000
Lithuanian passport	\$1,500
Maltese Passport	\$6,500
Maltese Passport	\$6,500
Various European Union passports	\$4,000

WHY THIS IS IMPORTANT

Attack programs do not need to be developed, ready-made ones can be found on the market

WHY THIS IS IMPORTANT

Malware	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Global low quality, slow speed, low success rate x 1000	\$70	\$50	-\$20
Europe low quality, slow speed, low success rate x 1000	\$300	\$320	+\$20
USA, CA, UK, AU low quality, slow speed, low success rate x 1000	\$800	\$900	+\$100
Global med quality, 70% success rate x 1000	\$80	\$80	-
Europe med quality, 70% success rate x 1000	\$700	\$500	-\$200
USA only med quality, 70% success rate x 1000	\$900	\$1,000	+\$100
USA, CA, UK, AU med quality, 70% success rate x 1000	\$1,300	\$1,400	+\$100
Europe fresh high quality x 1000	\$2,300	\$2,500	+\$200
Europe aged high quality x 1000	\$1,400	\$1,200	-\$200
USA high quality x 1000	\$1,700	\$1,900	+\$200
CA high quality x 1000	\$1,500	\$1,400	-\$100
UK high quality x 1000	\$2,000	\$2,200	+\$200
Android x 1000	\$600	\$900	+\$300
Premium x 1000	\$6,000	\$5,000	-\$1,000

DDOS Attacks	Avg. Price USD (2020)	Avg. Price USD (2021)	YoY Difference
Unprotected website, 10-50k requests per second, 1 hour	\$10	\$15	+\$5
Unprotected website, 10-50k requests per second, 24 hours	\$60	\$50	-\$10
Unprotected website, 10-50k requests per second, 1 week	\$400	\$500	+\$100
Unprotected website, 10-50k requests per second, 1 month	\$800	\$1,000	+\$200
Premium protected website, 20-50k requests per second, multiple elite proxies, 24 hours	\$200	\$200	-

WHAT ARE THE BENEFITS OF DARKSOC® ?

DARKSOC® as a Service

- Increases cyber intelligence capabilities
- Anticipates constantly changing cyberworld (early warnings)
- Complements the company's cyber maturity
- Serves as a forensic investigation tool
- Supports organisational strategic decision-making
- Complements the strategic cyber situational awareness
- Discovers vulnerabilities and weaknesses
- Facilitates the cyber strategy process

→ **BETTER CYBER SECURITY CAPABILITY AND RESILIENCE**





DARKSOC® CREATES BETTER CYBER SECURITY CAPABILITIES AND RESILIENCE.



CYBERWATCH FINLAND

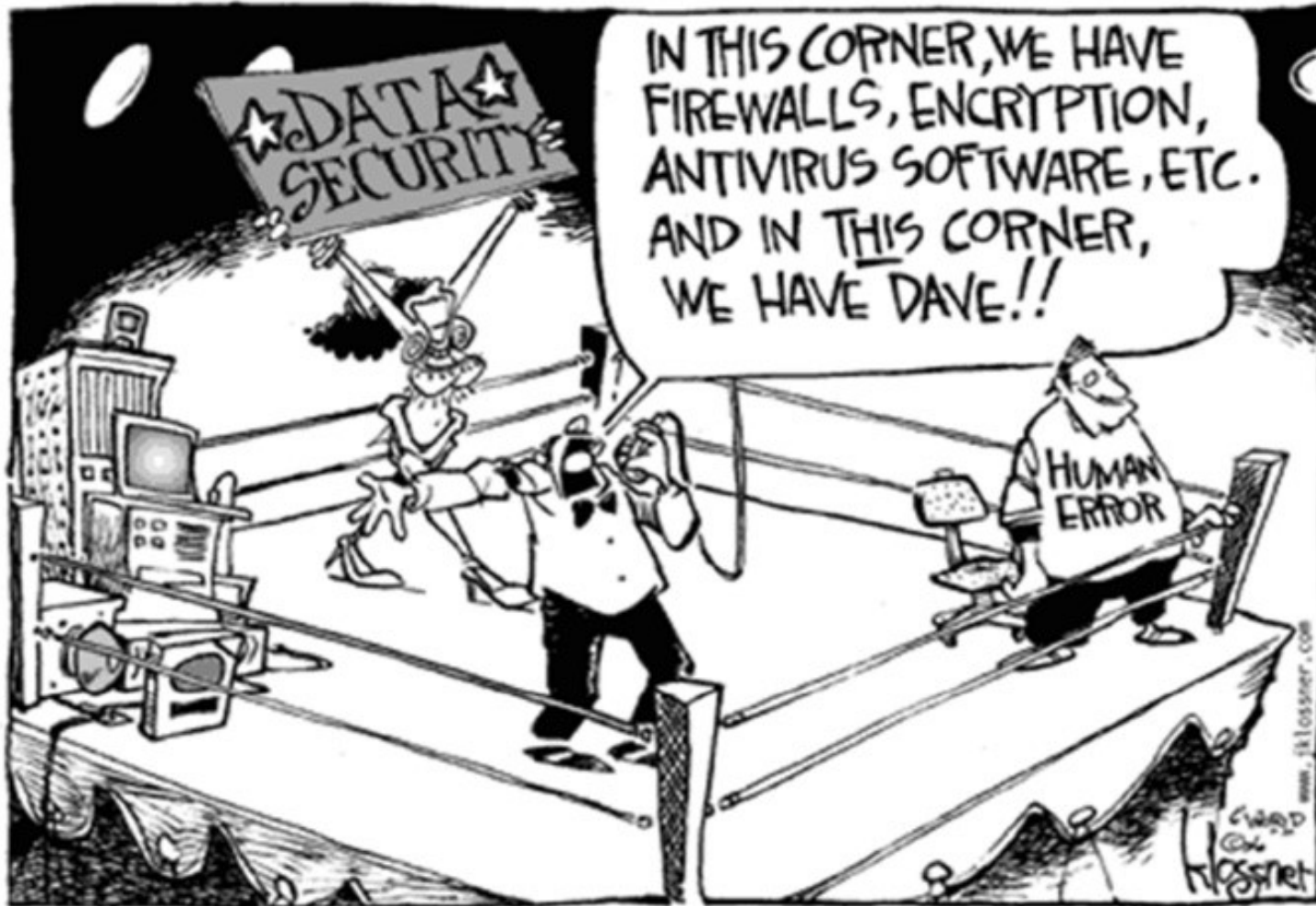
PREPARE

- Attacking Anonymous and other groups is illegal.
- What can companies and organizations do to prepare?
- Check if ict assets displayed on the Internet have been identified, scanned, patched or placed behind a firewall?
- Track password leaks, still the most common attack vector from the dark web side.
- Backup, recovery from faults.

			
BTC Clipper BTC Stealer BTC Grabber Build...	Phoenix Keylogger	MarsStealer V3 + panel + Builder	Azorult Stealer v3.4
7.99 USD	9.99 USD	45 USD	35 USD
Steal BTCs Features Startup/Install Icon Changer Assembly Editor EXE Builder	Features: Keylogger + Clipboard Stealer Screen Capture Password Stealing (Browsers, Mail Clients, FTP clients, Chat Clients) Data exfiltration via SMTP...	What info does it steals you can see in my other listing. Browsers: Internet Explorer, Microsoft Edge Google Chrome, Chromium, Microsoft Edge (Chromium ve...	What info does it steals you can see in my other listing. Stealer of saves passwords from: Mail clients • Outlook • Thunderbird FTP clients • Filezilla...

HUMAN FACTOR

40%



60%

COMPETENCE DEVELOPMENT

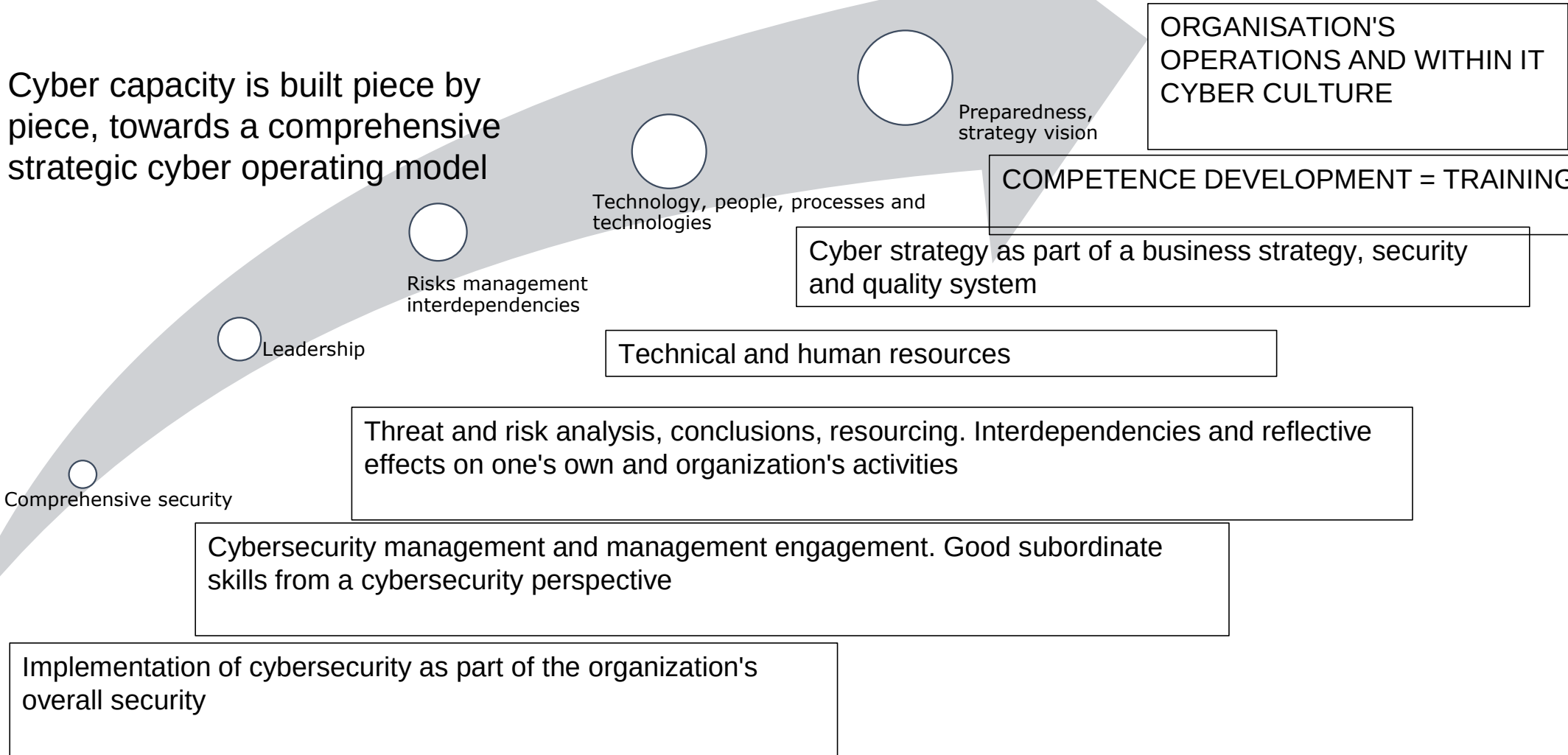
National cyber security competence will be ensured by identifying requirements and strengthening education and research.

- At the national level, it must be ensured that companies have both top-level experts and other competent personnel.



CYBER CAPACITY BUILDING (CCB)

Cyber capacity is built piece by piece, towards a comprehensive strategic cyber operating model





In the world of cyber security

CYBERWATCH FINLAND



IN THE WORLD OF CYBER SECURITY

WHY IS FORESIGHT IMPORTANT?

CYBERWATCH FINLAND

In the world of cyber security – Why is foresight important?

- Foresight is important because every company must create a strategy for itself, which is often used to prepare for changes outside of its own industry.
- To support decision-making, we need to know what phenomena, trends and megatrends are emerging and what future surprises could be those that affect the security of our operating environment and the continuity of our businesses.
- Living in the midst of change requires both comprehensive vision and knowledge.
- What kind of developments are visible, how could they relate to each other, and how could their combined impact on future changes could be predicted?
- The future is uncertain.
- The only thing we know for sure is what is happening in the present, but by looking at the present systematically, we can reliably say something about the future.
- The models created with the help of foresight in turn help us to draw conclusions and based on these conclusions, we can choose certain actions to prepare for different futures.

That is why foresight is important.

A nighttime photograph of a city street. In the foreground, a multi-lane highway with a concrete barrier runs across the frame. To the left, a parking lot is filled with cars. In the background, several tall buildings are illuminated, including one with a sign that reads 'THEATRE'. Streetlights cast a warm glow over the scene.

IN THE WORLD OF CYBER SECURITY

WHAT CAN WE ACHIEVE WITH FORESIGHT?

CYBERWATCH FINLAND

In the world of cyber security – What can we achieve with foresight?

The transformation of global order!

- It is impossible to predict the future if you do not understand the environment in which we operate.
- From frightened reactions to proactive preparedness
- Instead of coming up with a static solution to respond to the crisis, we need to move towards a dynamic, proactive, ever-evolving approach and operating model with a solid understanding of where the cyber world is headed in the upcoming decades. It is important to ensure that one maintains a balanced understanding of all potential threats and disruptions, and make sure that one's organisation is well-prepared in advance.

FUTURES PLATFORM AND CYBERWATCH FINLAND

Futures Platform, the industry standard source for future trends and foresight, and Cyberwatch Finland, a leading cyber security advisory, have joined their forces in producing foresight analysis on cyber threats and security, as well as digital space in general.

Collaboration between future researchers and cybersecurity experts creates a proactive picture of the future of the cyber world.

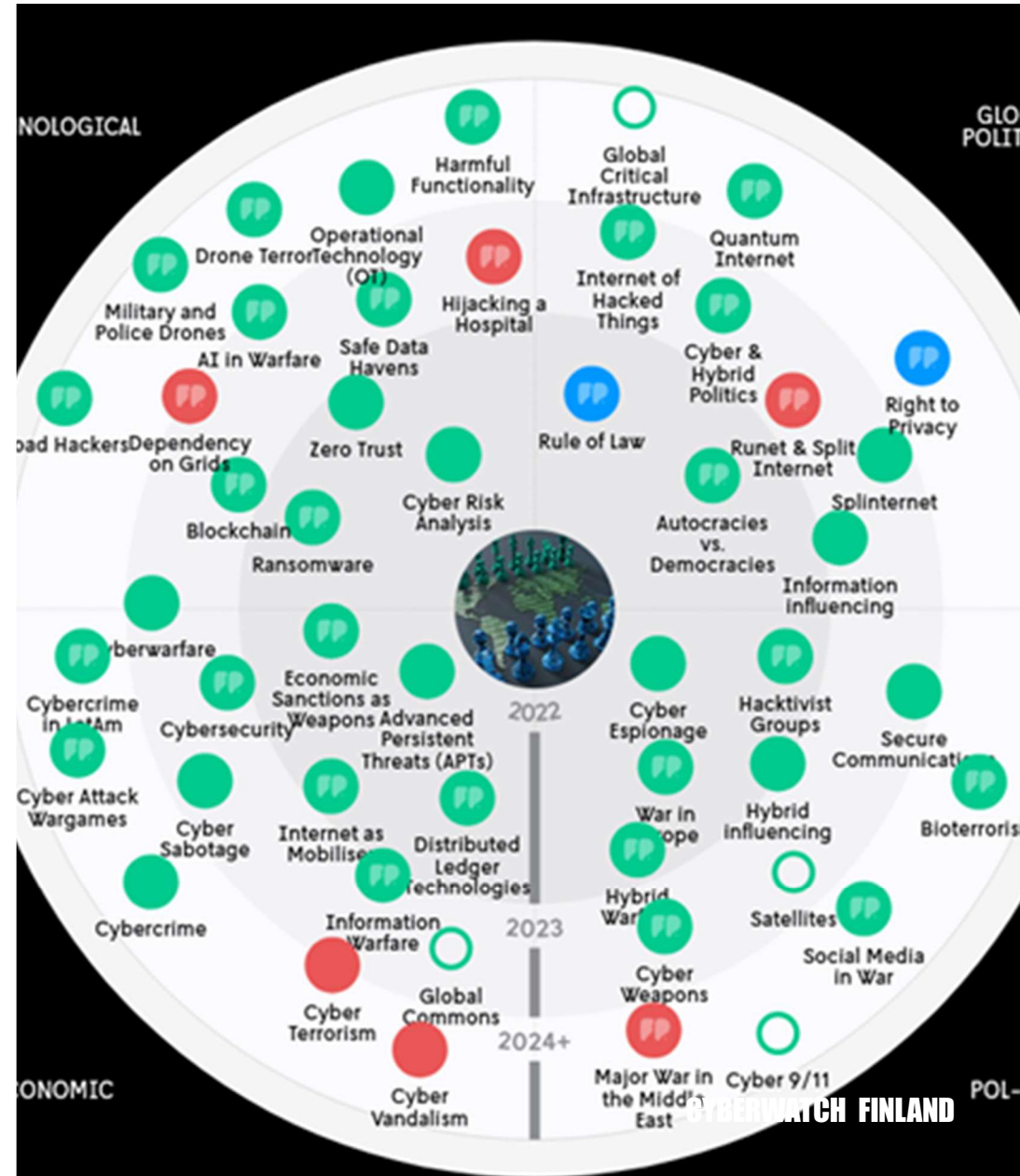


The reality of cybersecurity has evolved from an old-world two-dimensional one to a multi-purpose dynamic part of our lives with several ever-changing dimensions- some of which are even invisible...

- complexity and interdependencies have multiplied
- the rate of change has increased
- predictability has declined

In the present, and above all in the new world, cyber security is an essential part of creating opportunities for sustainable development and growth.

Proactive cyber security is a key premise for all responsible and legal actions.



ABOUT FUTURES PLATFORM

Futures Platform is the industry standard source for future trends, scenarios and long term change. It's a full-functionality visual and collaborative toolbox for foresight and management teams, ensuring your organisation's strategy and key decisions are future proof.

The solution brings together an AI-powered digital platform and the expertise of professional futurists. At its core, the platform features more than 800 analyses of future phenomena – from technological and environmental to societal change, with a focus on the long term. These compact, easy-to-digest scenario descriptions are combined with auto-crawled additional information from validated sources.

If you would like to know more head to <https://www.futuresplatform.com/>



CYBERWATCH FINLAND



THANK YOU !

CYBERWATCH FINLAND

perti@cyberwatchfinland.fi
Meritullinkatu 33
FI-00170 Helsinki FINLAND
www.cyberwatchfinland.fi