ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Knowledge-Sharing Webinar: Paradigm shift from cybersecurity to cyber resilience

July 22nd 2024

Agenda

ECCO
European Cybersecurity COmmunity

- **Objectives of the Webinar (5 Min)**
- **Cyber Risk Management as a Basis for Cyber Resilience (20 min).**
  - **Gabrijela Dreo Rodosek. Bundeswehr University Munich**
- **Impact of Generative AI on Cybersecurity (20 min).**
  - **Nad, Tomislav (Graz). SGS**
- **Open Q&A and discussion (15 min)**

ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Introduction

Antonio Skarmeta

July 22nd 2024

ECCO Community Working Groups

- Road-mapping
- Startups/Scaleups - SMEs support
- Human factors
- Skills
- Synergies on cybersecurity for Civilian and Space applications
- **Trusted supply chains**
  - **Chairs: Antonio Skarmeta and José Luis Hernández Ramos**
  - Participants: development of a "proto-community" based on the initial list of experts from ECSO and Pilots, and growing with additional people (44 members so far)
  - Objectives
    - Build community of experts on trusted supply chains and Strengthening Trusted and Resilient Supply Chain in Europe
    - Facilitate trusted information sharing about threats (to support prevention and response) and link to CISOs and SOCs
    - Propose a strategy, planning and recommendations to support the NCCs in the implementation of the Strategic Agenda's Action Plan

Paradigm shift from cybersecurity to cyber resilience

- Webinar today focused on the cyber resilience aspects in the supply chain
  - Analysis of the impact and relevance of the AI-based risk management
  - Shift from "static" cybersecurity approaches towards more "dynamic"
  - How AI support cyber defence as well as generate sophisticated and targeted cyber attacks
  - Impact of the Generative AI in transforming the cybersecurity landscape
  - Need to be prepared for AI-driven cyber threats approaches

Planned webinars

- This event is part of a webinar series focused on European cybersecurity supply chain.

- List of webinars
  - Organisational and Operation Security in Trusted Supply Chains
  - Certification in the lifecycle
  - Securing the Cyber Supply Chain: Lessons learned, Standards, and Strategies for mitigating modern Threats
  - Today → Paradigm shift from cybersecurity to cyber resilience
  - September: Methodology and gap analysis of actual standard covering the supply chain

ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Thanks and Enjoy the Webinar

Antonio Skarmeta

July 22nd 2024

ECCO
European Cybersecurity COmmunity

Impact of Generative AI on Cybersecurity

Navigating the Double-Edged Sword

Tomislav Nad, 11.07.2024

Cybersecurity and artificial intelligence

Generative AI is transforming the cybersecurity landscape.

It offers innovative defenses and predictive insights while simultaneously enabling more sophisticated and deceptive cyber attacks.

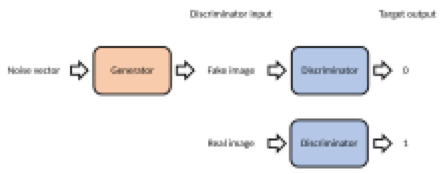
What is generative AI?

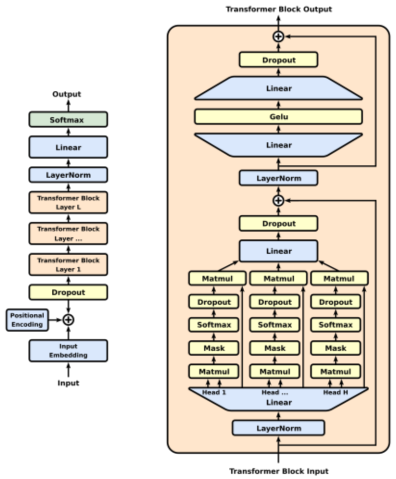
Definition: Generative AI refers to a class of artificial intelligence models that can generate new content based on the data they have been trained on. These models can create text, images, audio, or other data.

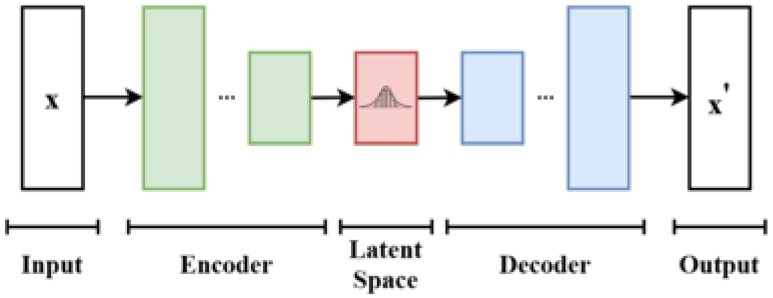
Generative Adversarial Networks (GANs): Consist of two neural networks, the generator and the discriminator, working in tandem to produce realistic data.

Generative Pre-trained Transformer (GPT): A type of language model capable of generating coherent and contextually relevant text based on a given prompt.

Variational Autoencoder (VAE): Learns a probabilistic representation of data to generate new, similar data samples while allowing for continuous and smooth variation.







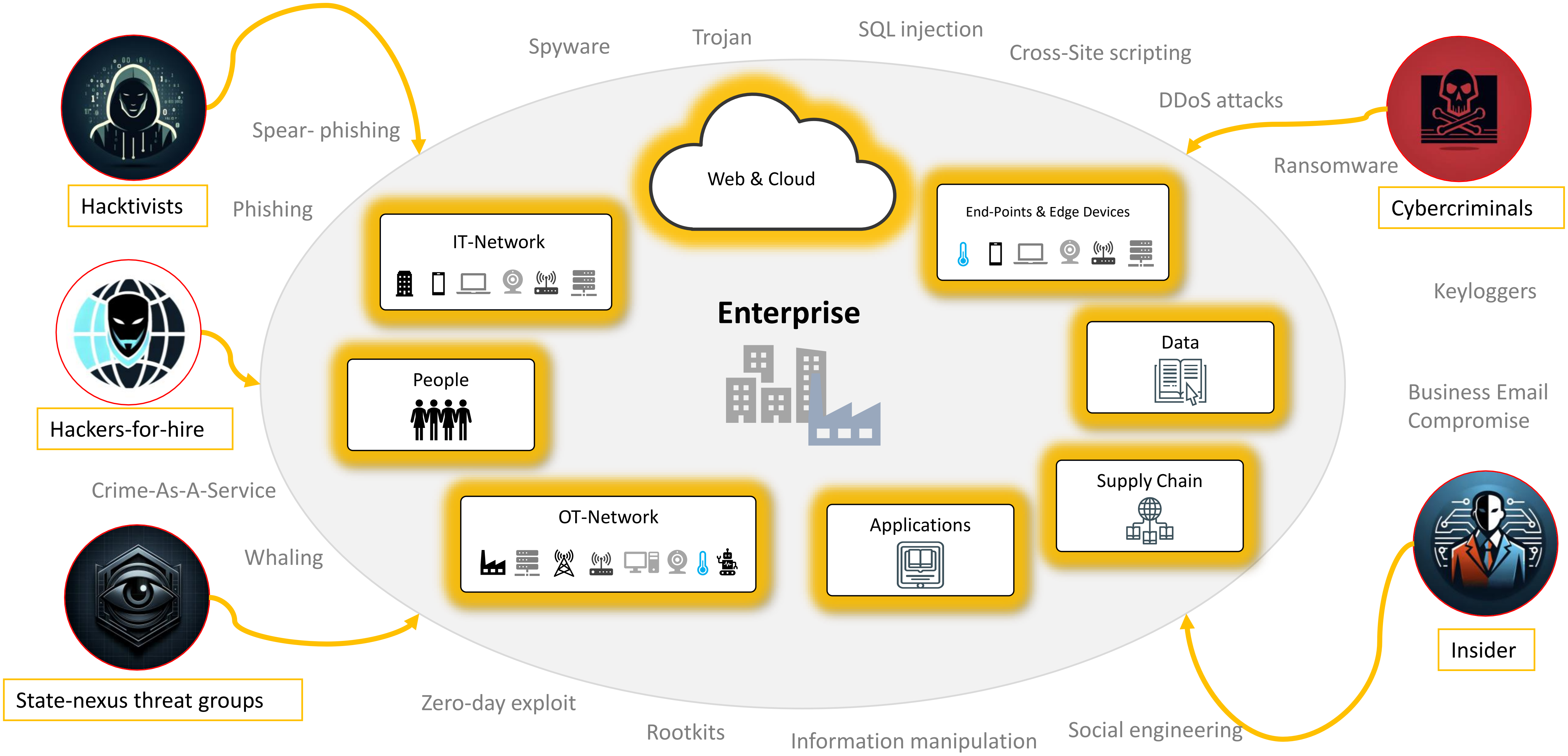
https://en.wikipedia.org/wiki/Generative_adversarial_network

https://en.wikipedia.org/wiki/Generative_pre-trained_transformer

https://en.wikipedia.org/wiki/Variational_autoencoder

Cybersecurity landscape: threats

ECCO European Cybersecurity COmmunity



Hacktivists

Hackers-for-hire

State-nexus threat groups

Cybercriminals

Insider

Spear- phishing

Phishing

Crime-As-A-Service

Whaling

Spyware

Trojan

SQL injection

Cross-Site scripting

DDoS attacks

Ransomware

Keyloggers

Business Email Compromise

Zero-day exploit

Rootkits

Information manipulation

Social engineering

Enterprise

Web & Cloud

IT-Network

End-Points & Edge Devices

People

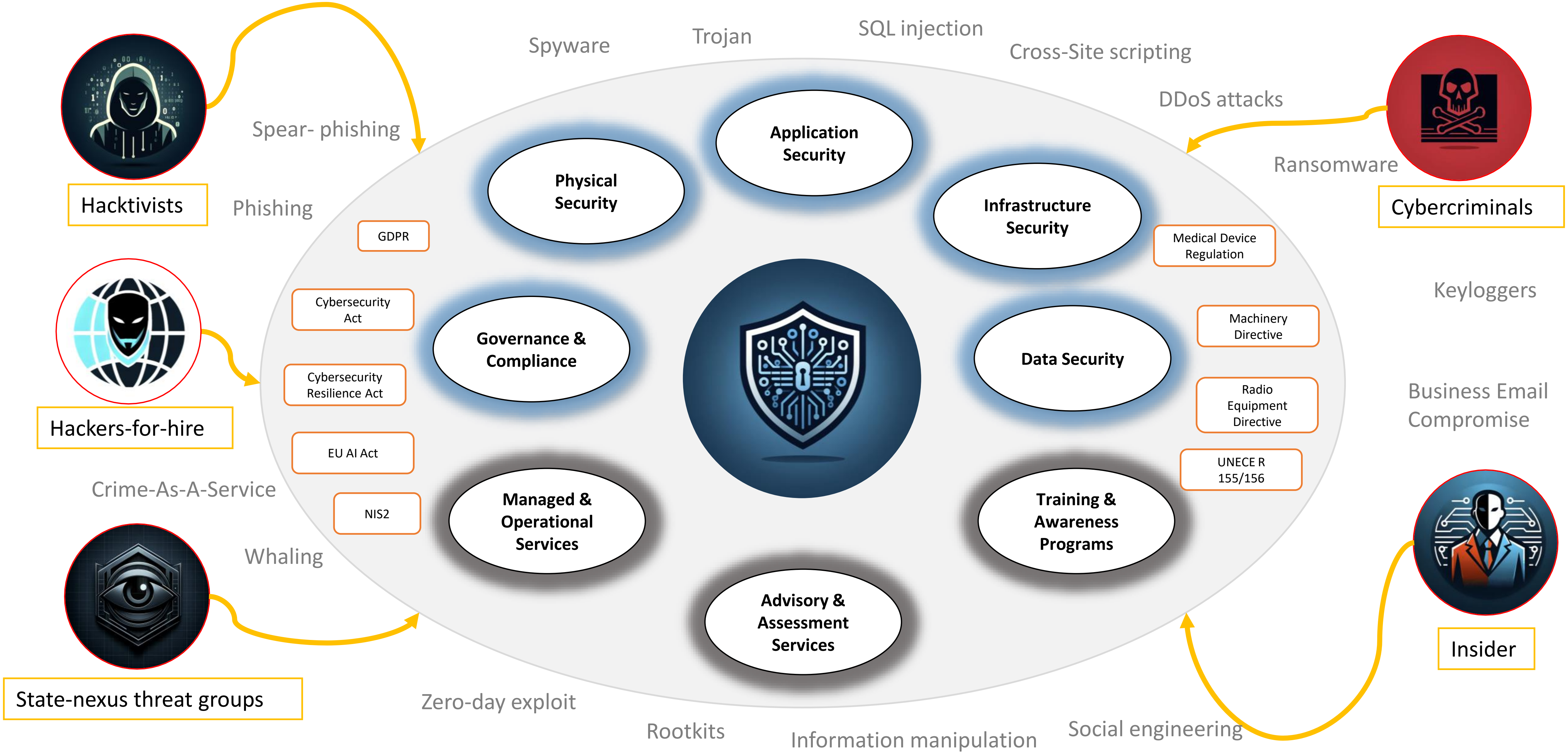
Data

OT-Network

Applications

Supply Chain

Cybersecurity landscape: eco system



Hacktivists

Hackers-for-hire

State-nexus threat groups

Cybercriminals

Insider

Spear- phishing

Phishing

Crime-As-A-Service

Whaling

Zero-day exploit

Rootkits

Information manipulation

Social engineering

Spyware

Trojan

SQL injection

Cross-Site scripting

DDoS attacks

Ransomware

Keyloggers

Business Email Compromise

Physical Security

Application Security

Infrastructure Security

Governance & Compliance

Data Security

Managed & Operational Services

Advisory & Assessment Services

Training & Awareness Programs

GDPR

Cybersecurity Act

Cybersecurity Resilience Act

EU AI Act

NIS2

Medical Device Regulation

Machinery Directive

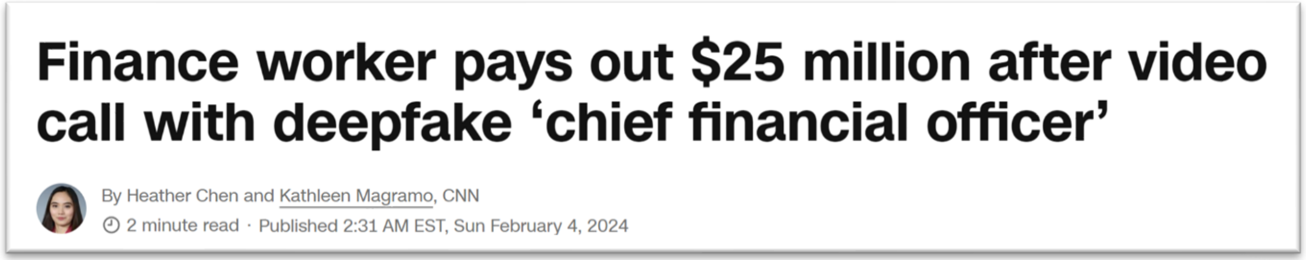
Radio Equipment Directive

UNECE R 155/156

Threats posed by generative AI

- **Creating sophisticated phishing attacks**
  - **Use case**: GenAI can be used by attackers to create highly convincing phishing emails and websites.
  - **Example**: Generating personalized phishing emails that are indistinguishable from legitimate communication, increasing the likelihood of successful attacks.
- **Developing polymorphic malware**
  - **Use case**: Attackers can use GenAI to create malware that constantly changes its code to avoid detection by traditional signature-based antivirus systems.
  - **Example**: Polymorphic malware that adapts its structure each time it infects a new system, making it harder for detection systems to identify and block it.
- **Generating malicious code**
  - **Use case**: GenAI can be used to generate code snippets for malware or exploit development.
  - **Example**: Providing attackers with detailed and functional code to exploit vulnerabilities or bypass security measures.
- **Creating deepfake content for social engineering**
  - **Use case**: GenAI can produce realistic audio and video deepfakes that can be used in social engineering attacks.
  - **Example**: Generating fake videos of executives instructing employees to transfer funds or disclose sensitive information.
- **Evasion techniques**
  - **Use case**: GenAI can create methods to bypass traditional cybersecurity defenses.
  - **Example**: Using GenAI to generated obfuscation techniques, evading detection algorithms.

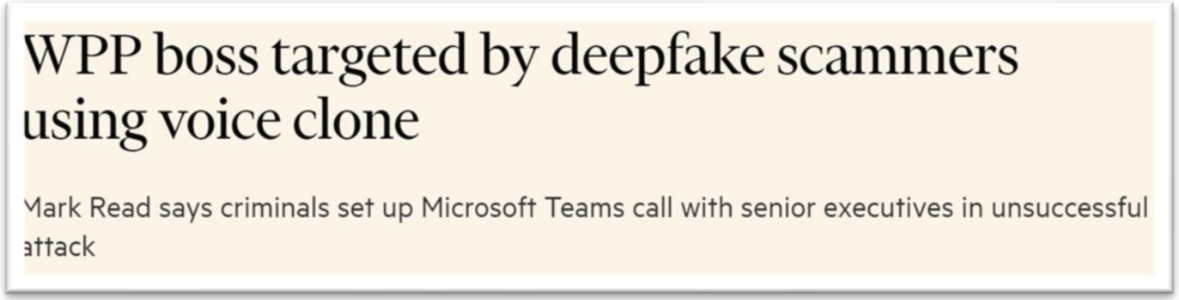
Examples



Finance worker pays out $25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html



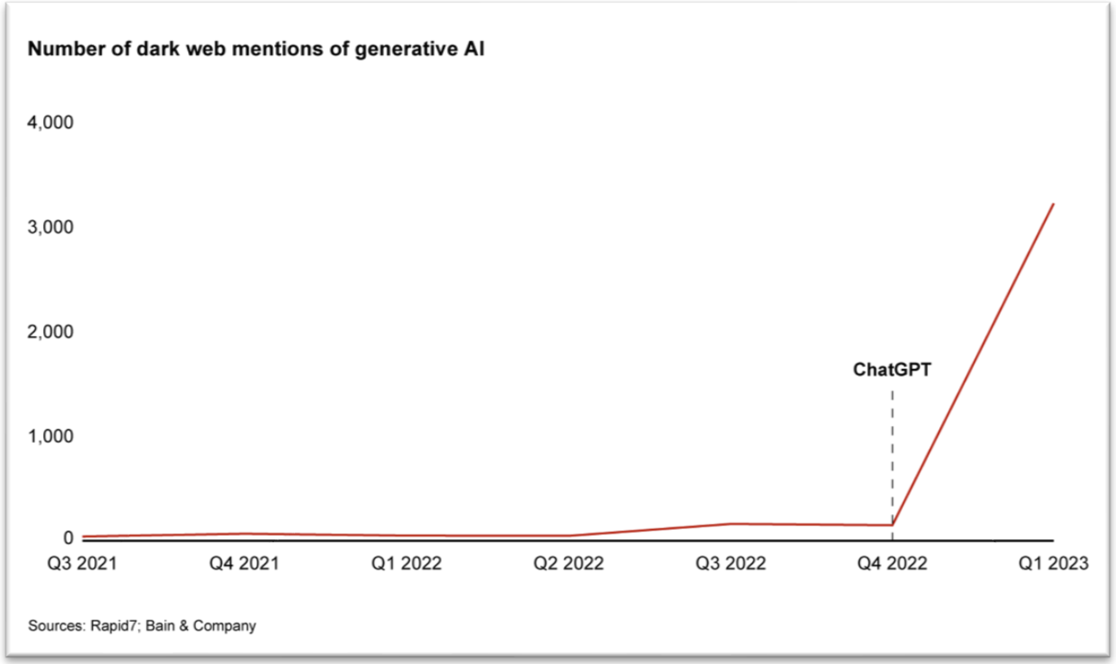
WPP boss targeted by deepfake scammers using voice clone

Mark Read says criminals set up Microsoft Teams call with senior executives in unsuccessful attack

https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0

How FraudGPT presages the future of weaponized AI

https://venturebeat.com/security/how-fraudgpt-presages-the-future-of-weaponized-ai/



Number of dark web mentions of generative AI

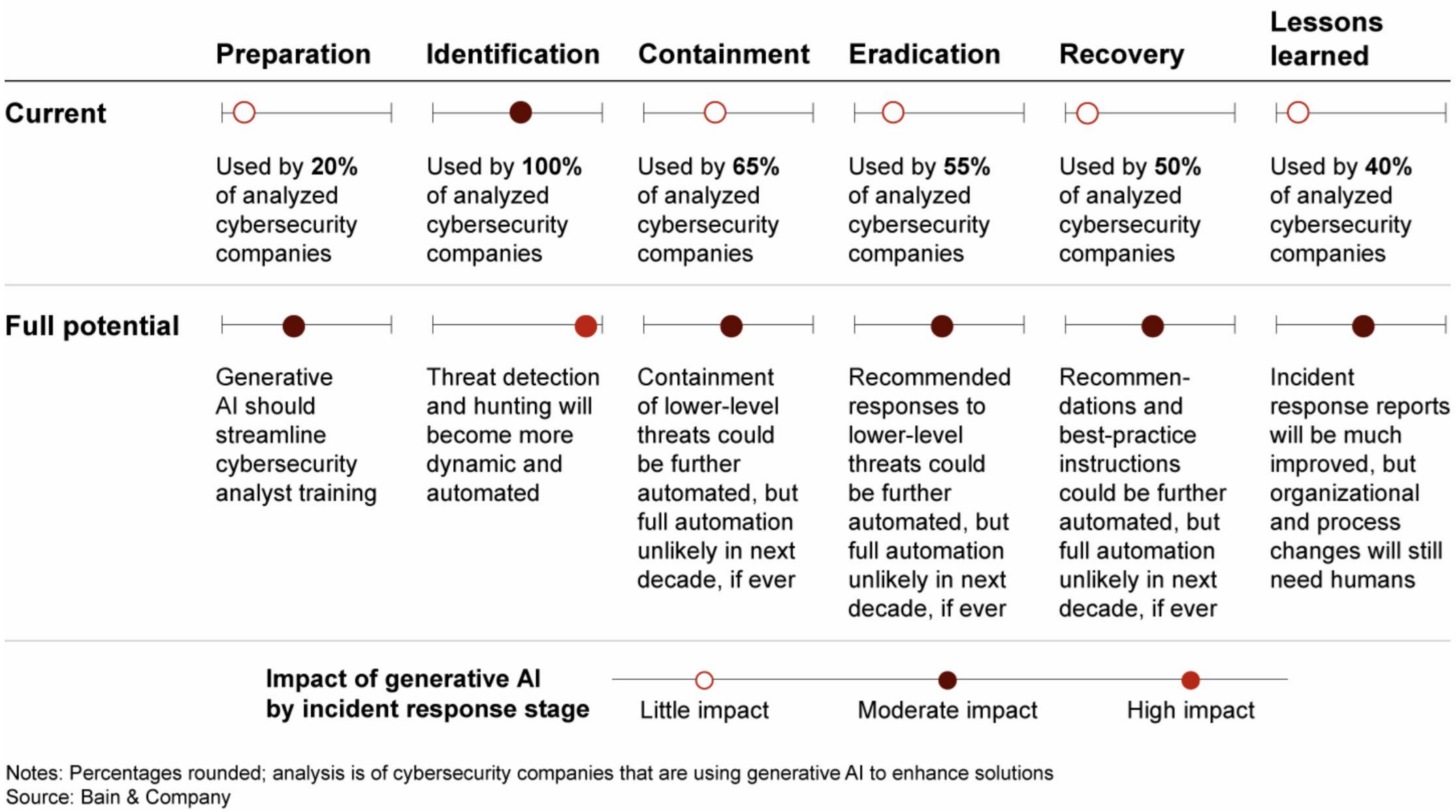
Sources: Rapid7; Bain & Company

https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/

Positive impacts of generative AI on cybersecurity

- **Automated threat intelligence**
  - **Use case**: GenAI can process and analyze vast amounts of threat intelligence data from various sources.
  - **Example**: Automatically summarizing threat reports, extracting indicators of compromise (IOCs), and generating alerts for security teams.
- **Anomaly detection**
  - **Use case:** GenAI can be used to detect unusual patterns in network traffic or user behavior that might indicate a cyber attack.
  - **Example**: A GAN-based system can generate synthetic network traffic data and compare it to actual network traffic to identify deviations that could signify intrusions.
- **Data augmentation for training**
  - **Use case**: GenAI can generate realistic synthetic data to augment training datasets for cybersecurity models.
  - **Example**: In situations where there is a lack of labeled data for training intrusion detection systems, GANs can create additional data to improve model accuracy.
- **Phishing detection**
  - **Use case**: GenAI can be used to generate a variety of phishing attack scenarios, which can then be used to train and improve detection systems.
  - **Example**: Creating a large dataset of phishing emails to train machine learning models to recognize and filter out phishing attempts more effectively.
- **Malware detection and evasion**
  - **Use case**: GenAI can generate malware samples that mimic real malware, helping in the development of robust detection systems.
  - **Example**: Training anti-malware tools on a diverse set of GAN-generated malware variants to enhance their ability to detect real-world malware.
- **Incident response automation**
  - **Use case**: GenAI can assist in drafting incident response plans and communications.
  - **Example**: Automatically generating detailed incident reports, response strategies, and communication templates during a cyber incident.

Usage of GenAI in incident response framework



	Preparation	Identification	Containment	Eradication	Recovery	Lessons learned
Current	○	●	○	○	○	○
	Used by **20%** of analyzed cybersecurity companies	Used by **100%** of analyzed cybersecurity companies	Used by **65%** of analyzed cybersecurity companies	Used by **55%** of analyzed cybersecurity companies	Used by **50%** of analyzed cybersecurity companies	Used by **40%** of analyzed cybersecurity companies
Full potential	●	🔴	●	●	●	●
	Generative AI should streamline cybersecurity analyst training	Threat detection and hunting will become more dynamic and automated	Containment of lower-level threats could be further automated, but full automation unlikely in next decade, if ever	Recommended responses to lower-level threats could be further automated, but full automation unlikely in next decade, if ever	Recommendations and best-practice instructions could be further automated, but full automation unlikely in next decade, if ever	Incident response reports will be much improved, but organizational and process changes will still need humans

Impact of generative AI by incident response stage

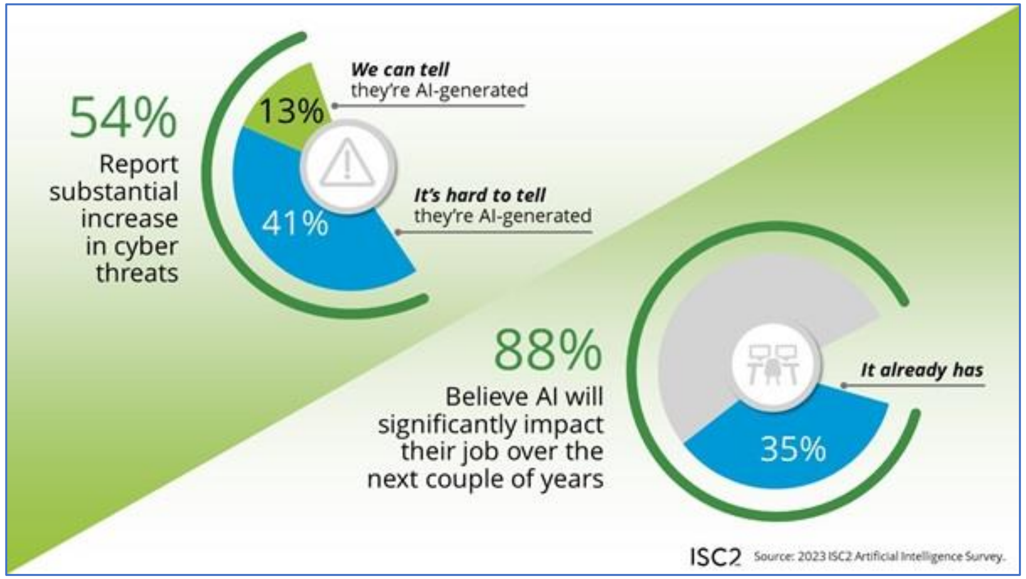
○	●	🔴
Little impact	Moderate impact	High impact

Notes: Percentages rounded; analysis is of cybersecurity companies that are using generative AI to enhance solutions
Source: Bain & Company

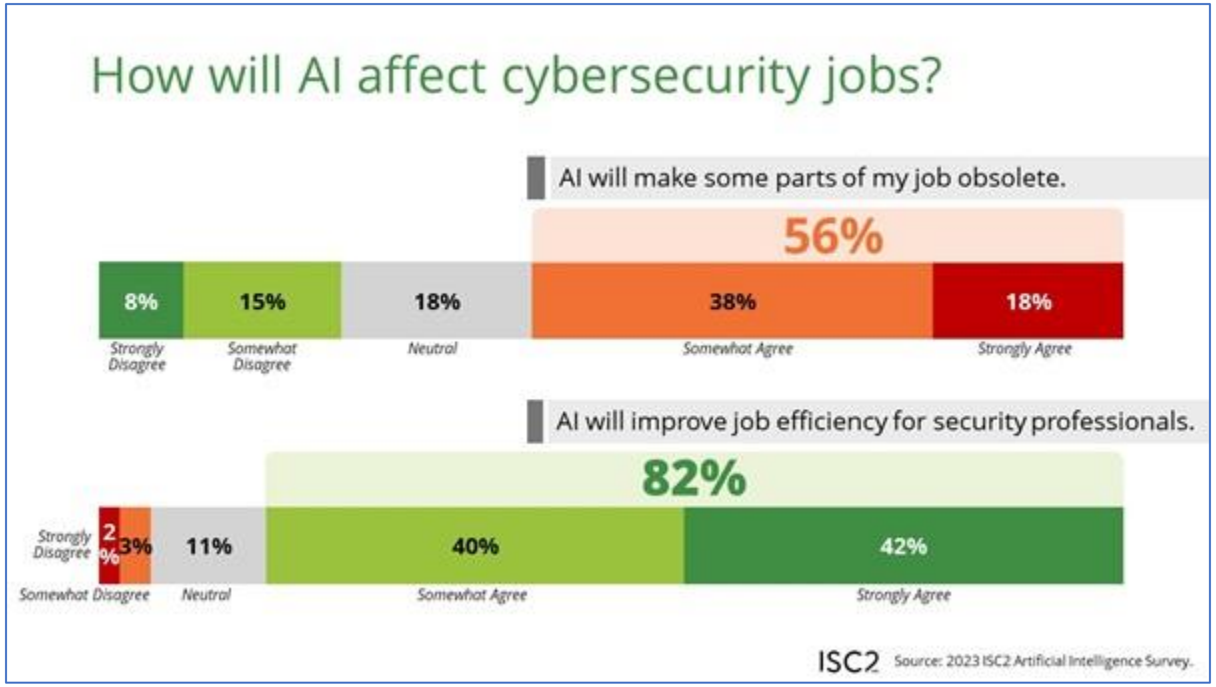
https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023/

Real-world impact of AI on cybersecurity professionals

ECCO European Cybersecurity COmmunity



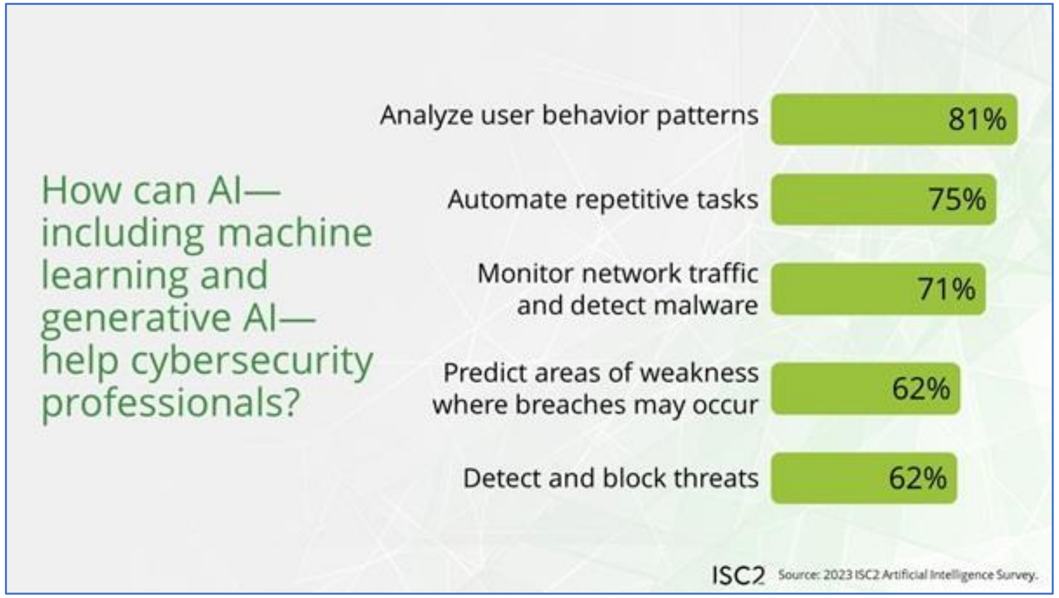
Source: 2023 ISC2 Artificial Intelligence Survey.



Source: 2023 ISC2 Artificial Intelligence Survey.

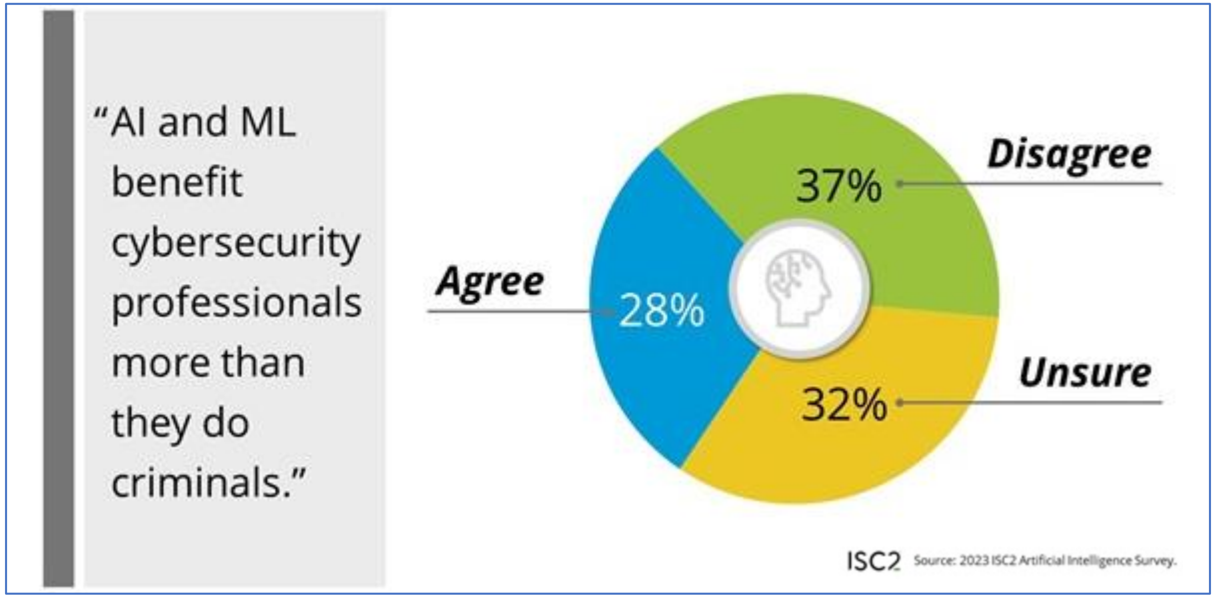
https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

Real-world impact of AI on cybersecurity professionals



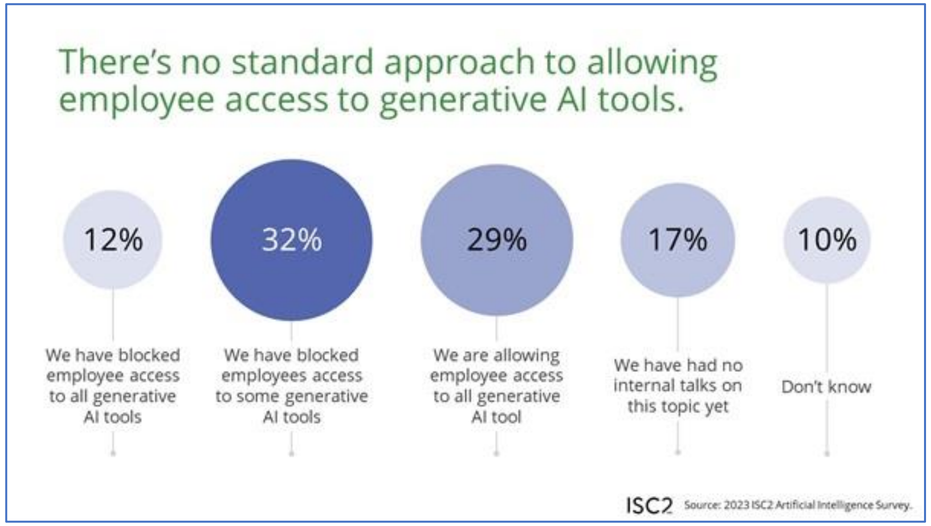
How can AI—including machine learning and generative AI—help cybersecurity professionals?

ISC2 Source: 2023 ISC2 Artificial Intelligence Survey.



"AI and ML benefit cybersecurity professionals more than they do criminals."

ISC2 Source: 2023 ISC2 Artificial Intelligence Survey.



There's no standard approach to allowing employee access to generative AI tools.

ISC2 Source: 2023 ISC2 Artificial Intelligence Survey.

https://www.isc2.org/Insights/2024/02/The-Real-World-Impact-of-AI-on-Cybersecurity-Professionals

Key take aways (1/4)

Dual Nature of Generative AI

- Generative AI offers powerful capabilities for both enhancing and undermining cybersecurity.
- It can be leveraged for advanced threat detection, data augmentation, and anomaly detection, while also posing risks through sophisticated phishing, deepfakes, and polymorphic malware.

Key take aways (2/4)

Mitigation Strategies

- Implementing AI in defense strategies, promoting ethical AI development, and fostering collaboration are crucial steps in mitigating risks.
- Continuous education, adaptive defense mechanisms, and proactive policies are essential for staying ahead of evolving threats.

Key take aways (3/4)

Future Trends

- Generative AI will continue to advance, bringing both opportunities and challenges to the cybersecurity landscape.
- Companies and professionals must be prepared for AI-driven cyber threats by adopting innovative solutions and maintaining a proactive approach.

Key take aways (4/4)

Professionals and Companies

- Cybersecurity professionals should stay informed, adopt advanced AI tools, and advocate for ethical AI use.
- Companies should invest in AI-driven security solutions, implement comprehensive security policies, and foster a security-first culture.

Contact

tomislav.nad@sgs.com

https://www.linkedin.com/in/tomislavnad/

www.sgs.com/

From Cyber Security to Cyber Resilience: A Paradigm Shift

Prof. Dr. Gabi Dreo Rodosek

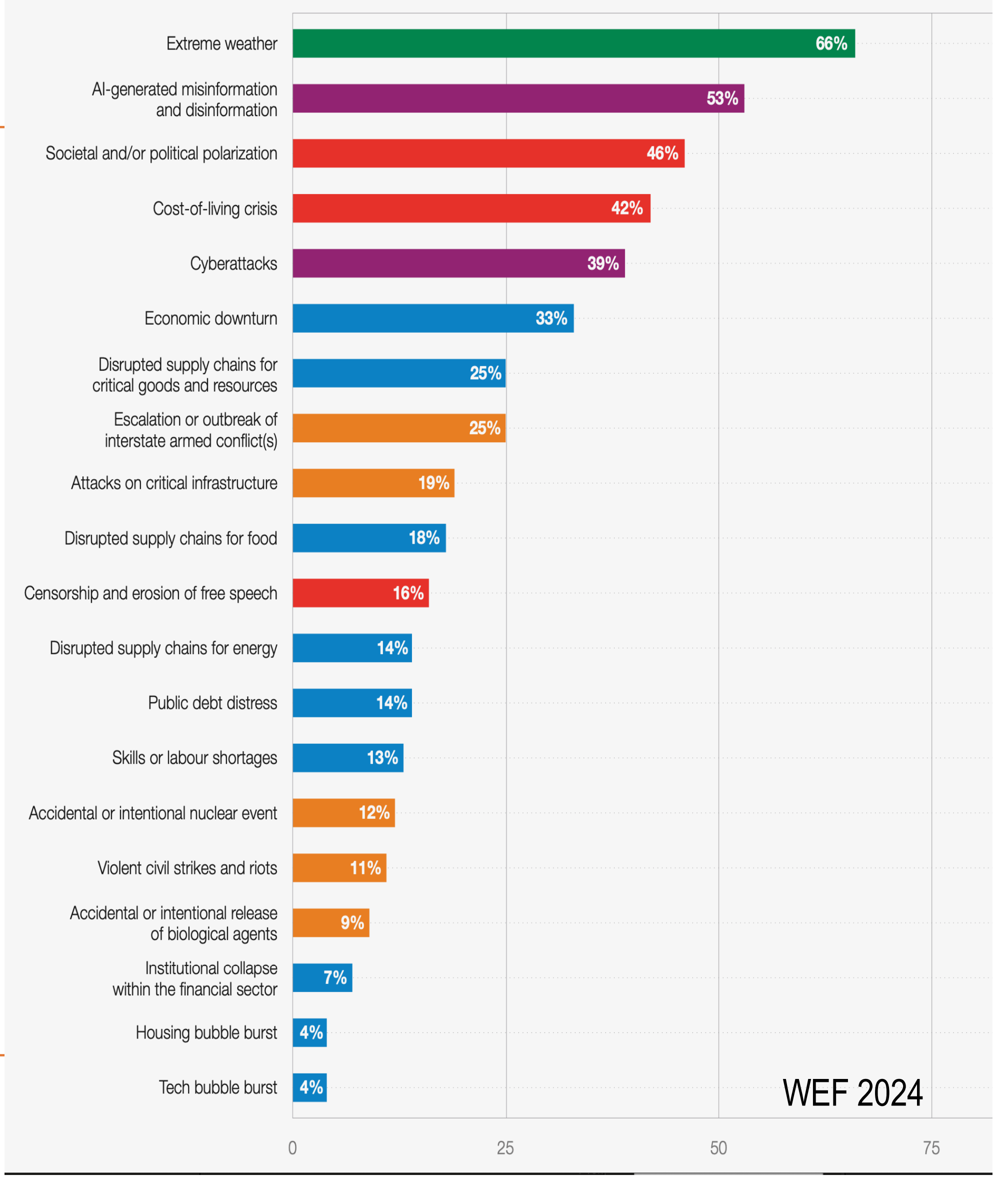
Chair for Communication Systems and Network Security

University of the Bundeswehr Munich

gabi.dreo@unibw.de

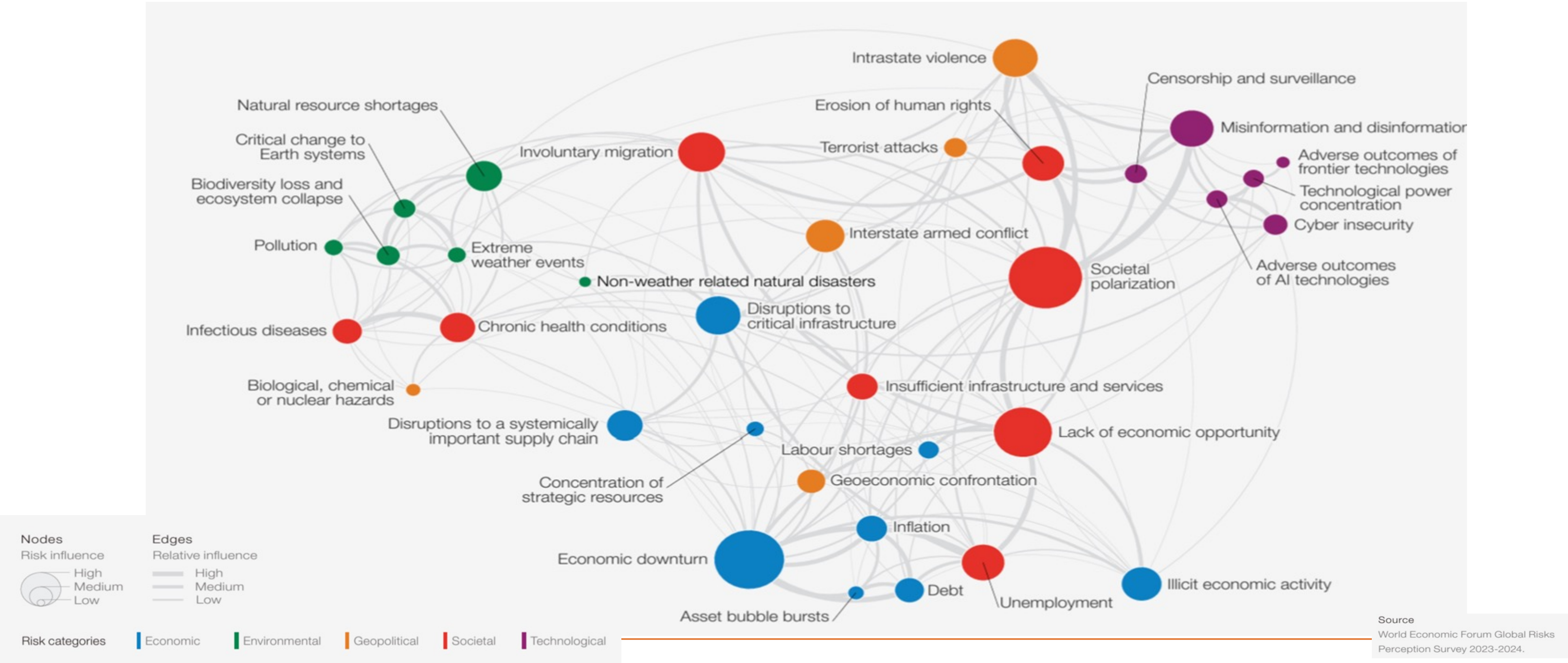
Increasing Threat/Risk Landscape

Growing geopolitical tensions
Rising economic uncertainty
Rapidly advancing technologies
Highly dynamical risk landscape
Evolving regulatory landscape
(national, international)



WEF 2024

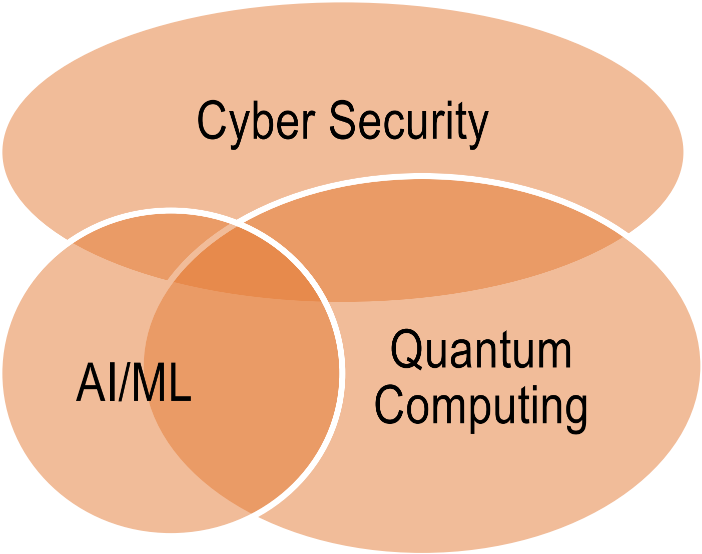
Risks and Risk Dependencies are Changing through Time and Volume


Intrastate violence
Censorship and surveillance
Natural resource shortages
Erosion of human rights
Misinformation and disinformation
Critical change to Earth systems
Involuntary migration
Terrorist attacks
Adverse outcomes of frontier technologies
Biodiversity loss and ecosystem collapse
Technological power concentration
Cyber insecurity
Interstate armed conflict
Pollution
Extreme weather events
Societal polarization
Adverse outcomes of AI technologies
Non-weather related natural disasters
Disruptions to critical infrastructure
Infectious diseases
Chronic health conditions
Insufficient infrastructure and services
Biological, chemical or nuclear hazards
Disruptions to a systemically important supply chain
Lack of economic opportunity
Labour shortages
Concentration of strategic resources
Geoeconomic confrontation
Inflation
Economic downturn
Debt
Illicit economic activity
Unemployment
Asset bubble bursts
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological

Source
World Economic Forum Global Risks Perception Survey 2023-2024.

GenAI vs. Quantum vs. Cyber Security

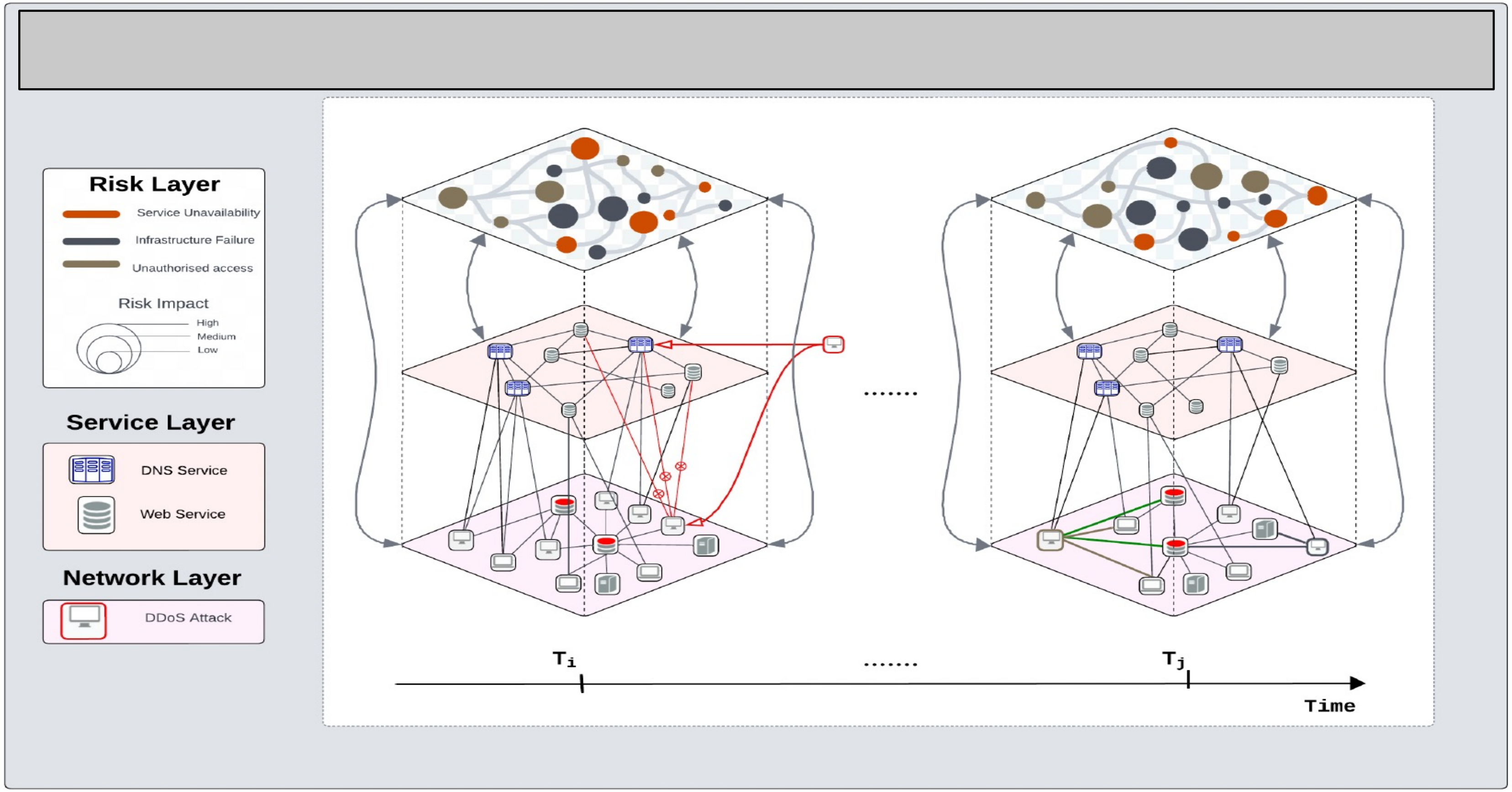
Generative AI: the Good and the Bad



New Attack Vectors

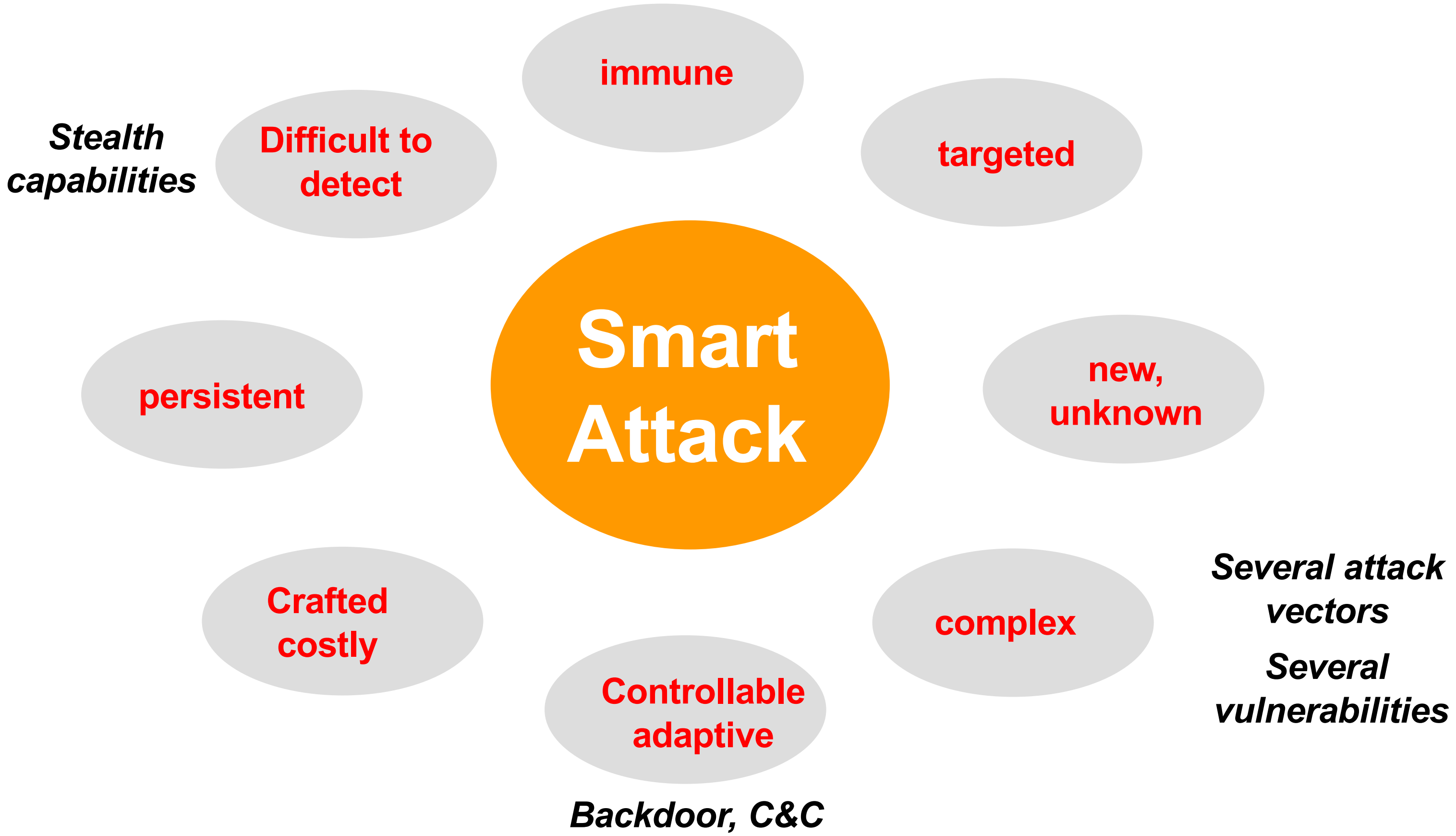
Quantum Threat
Quantum Resistant Encryption

Dependencies on the Risk/Service/Network Layer



... as IT is rapidly evolving ...
so are attacks ...

Towards Smart Attacks



What do we have Today: (Static) Cybersecurity

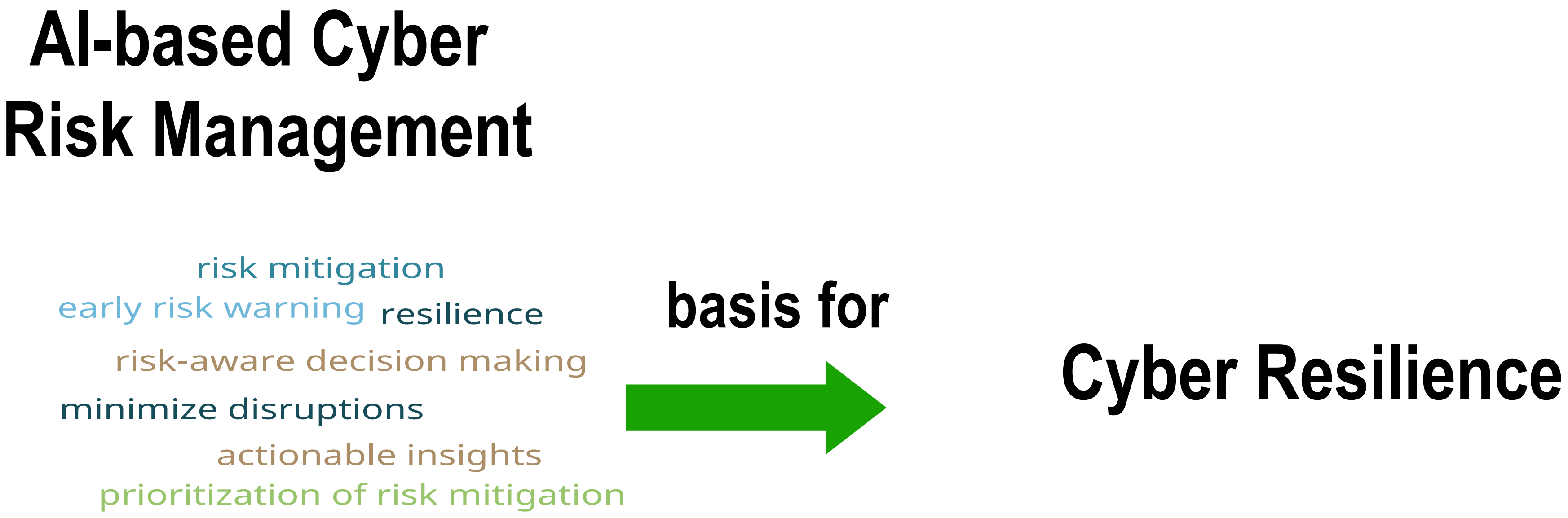
- Asymmetry of the attacks
- "Static" attack surface
- Reliance on rules and signatures („what we know“)
- Firewalls: yes, but how appropriate, updating of rules?
- Intrusion detection systems: yes, but static (signature-based)
- Anomaly-based systems: yes, but difficult to identify the "ground thruth" ...

„Never Change a Running System“ → *Not good*☺

What do we Need: Cyber Resilience

- Dynamization of the attack surface to eliminate attackes‘s asymmetric advantage of time
  - Approaches as Moving Target Defence
- Usage of GenAI/AI/ML to cope with the dynamics
  - Cybersecurity and AI
The Good and the Bad!
- Zero-trust (“Verify-All“)
- Zero-Touch Management
- ...

Towards a Risk-Based Cyber Resilience



AI-based Cyber Risk Management

risk mitigation

early risk warning resilience

risk-aware decision making

minimize disruptions

actionable insights

prioritization of risk mitigation

basis for

Cyber Resilience