ENISA
AI CYBERSECURITY CONFERENCE

7 June, Brussels

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

AI

Cybersecurity Trends: Opportunities and Threats for R&I

Rafael Popper

Director of Futures Diamond (UK) and Adjunct Professor at Finland Futures Research Centre (FFRC) of the University of Turku (FI)

FUTURES DIAMOND

FFRC

METHODOLOGY

Combining Methods From Different Knowledge Sources

Source: Popper et al. (2022)

Evidence stocktaking

(a) Scanning and review of key academic literature
(b) Identification and mapping Foresight Projects
(c) Review of ENISA projects
(d) Data analytics and extrapolation

Expertise

(a) Review of interviews with key AI stakeholders and experts to detect key/critical technologies and to validate identified trends
(b) Focus groups with foresight international experts
(c) Government, Business, Research and Civil Society panels

Interaction

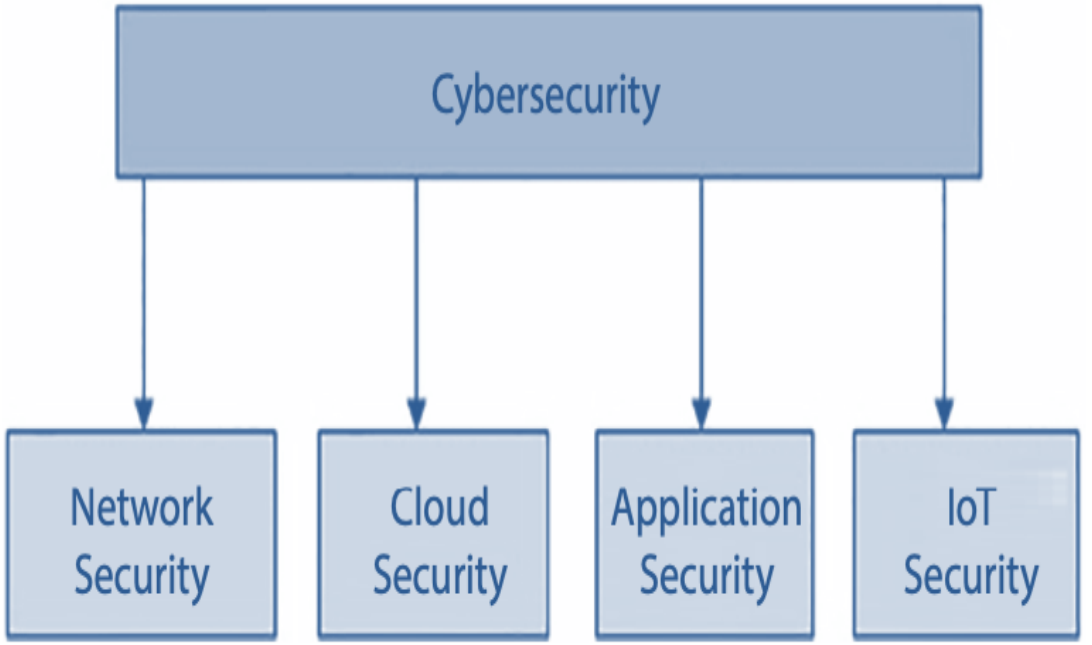
(a) Participation in relevant AI events and conferences, e.g., European Robotics Forum 2022 in Rotterdam
(b) Focus Groups and Roundtables with AI and foresight researchers, e.g., 2022 Foresight Executive Course in Manchester
(c) Sequential sessions of experts' roundtables

Creativity

(a) Review of scenario-based analysis of strengths, weaknesses, opportunities, and threats in relevant AI for cybersecurity future contexts
(b) Identification of wild cards in the scanned literature

CONCEPTS, MODELS & APPROACHES

Trends in Artificial Intelligence Research



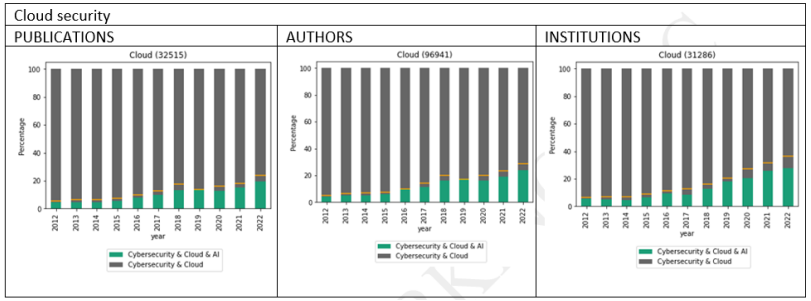
Source: Popper et al. (2022)

SEMI-AUTOMATED DATA MINING

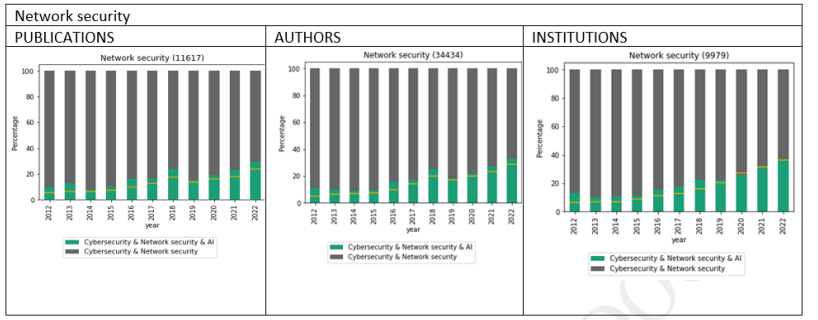
Publication and Conferences Dataset Analysis

274,108 publications on cybersecurity in the last 10y

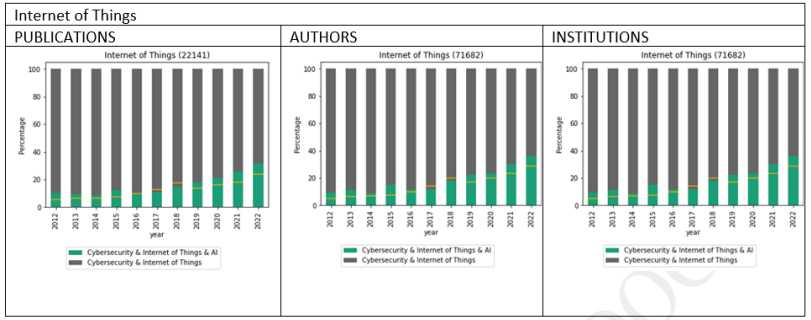
44,236 publications on cybersecurity + AI in the last 10y



CLOUD SECURITY



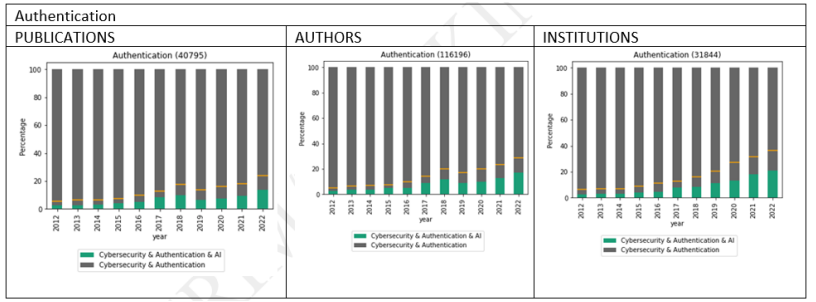
NETWORK SECURITY



IOT

MALWARE

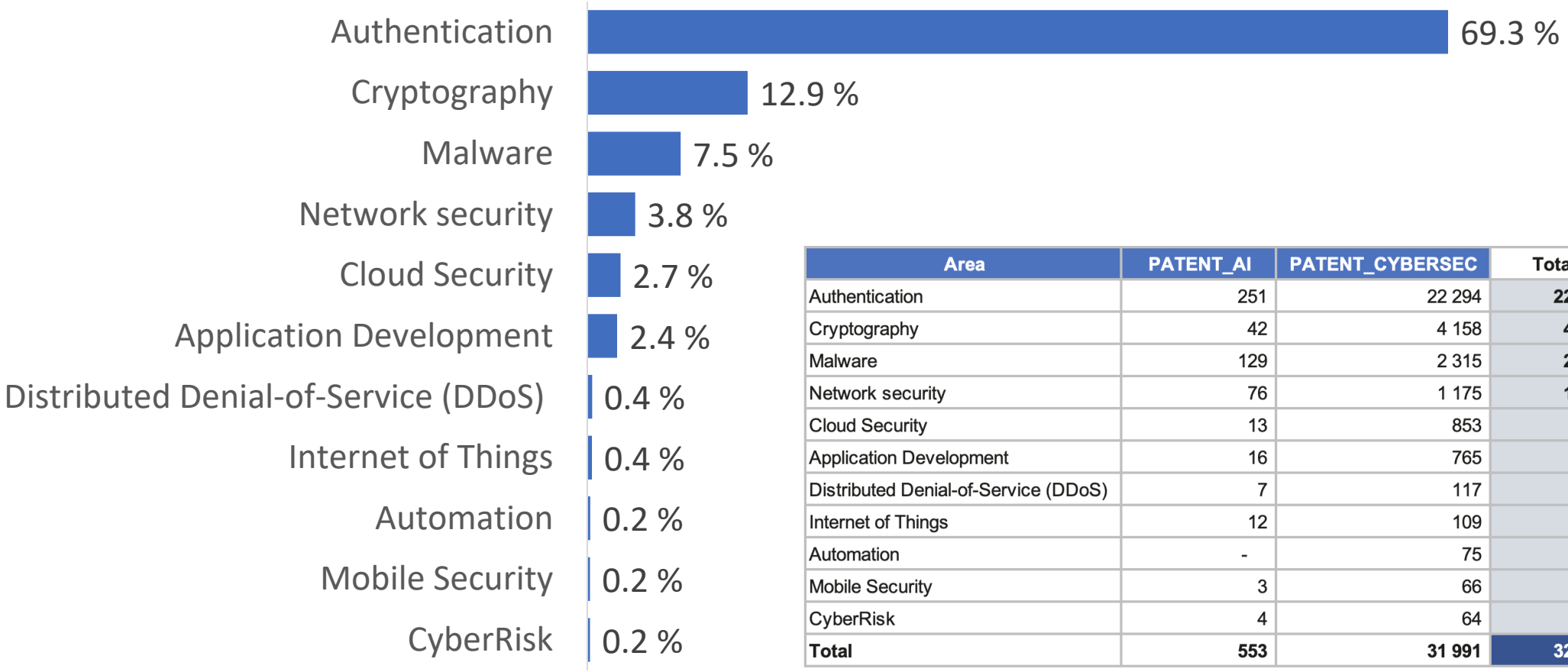
AUTHENTICATION



Source: Popper et al. (2022)

SEMI-AUTOMATED PATENT ANALYSIS

31,991 mention cybersecurity & 553 mention AI



Area	PATENT_AI	PATENT_CYBERSEC	Total	Percentage
Authentication	251	22 294	**22 545**	69,3 %
Cryptography	42	4 158	**4 200**	12,9 %
Malware	129	2 315	**2 444**	7,5 %
Network security	76	1 175	**1 251**	3,8 %
Cloud Security	13	853	**866**	2,7 %
Application Development	16	765	**781**	2,4 %
Distributed Denial-of-Service (DDoS)	7	117	**124**	0,4 %
Internet of Things	12	109	**121**	0,4 %
Automation	-	75	**75**	0,2 %
Mobile Security	3	66	**69**	0,2 %
CyberRisk	4	64	**68**	0,2 %
Total	**553**	**31 991**	**32 544**	**100 %**

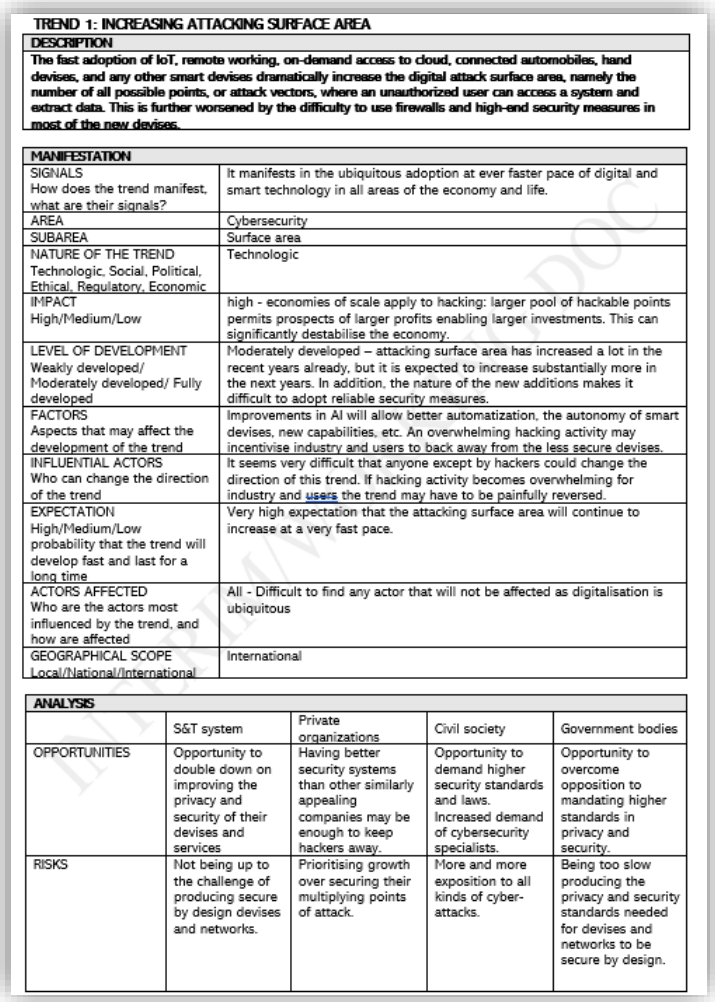
Source: Popper et al. (2022)

TREND CARDS

Trends in Artificial Intelligence Research

A **Trend Card** has been designed to provide:

- A description
- Manifestation profile
- Analysis of:
  - Opportunities
  - Risks



TREND 1: INCREASING ATTACKING SURFACE AREA

DESCRIPTION

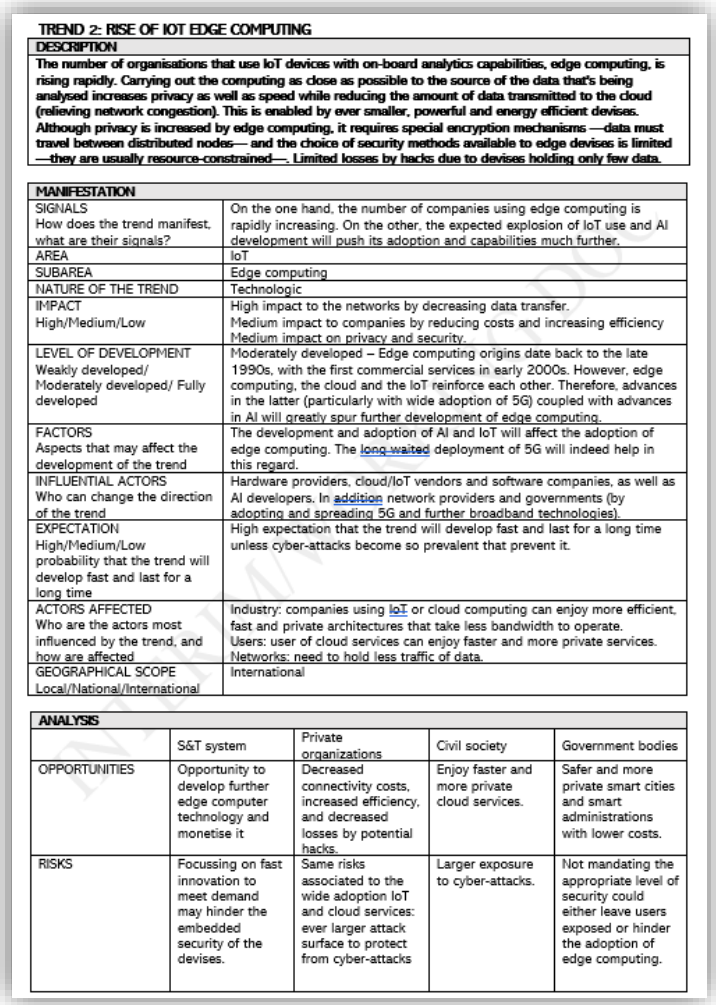
The fast adoption of IoT, remote working, on-demand access to cloud, connected automobiles, hand devises, and any other smart devises dramatically increase the digital attack surface area, namely the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. This is further worsened by the difficulty to use firewalls and high-end security measures in most of the new devises.

MANIFESTATION

SIGNALS How does the trend manifest, what are their signals?	It manifests in the ubiquitous adoption at ever faster pace of digital and smart technology in all areas of the economy and life.
AREA	Cybersecurity
SUBAREA	Surface area
NATURE OF THE TREND Technologic, Social, Political, Ethical, Regulatory, Economic	Technologic
IMPACT High/Medium/Low	high - economies of scale apply to hacking: larger pool of hackable points permits prospects of larger profits enabling larger investments. This can significantly destabilise the economy.
LEVEL OF DEVELOPMENT Weakly developed/ Moderately developed/ Fully developed	Moderately developed – attacking surface area has increased a lot in the recent years already, but it is expected to increase substantially more in the next years. In addition, the nature of the new additions makes it difficult to adopt reliable security measures.
FACTORS Aspects that may affect the development of the trend	Improvements in AI will allow better automatization, the autonomy of smart devises, new capabilities, etc. An overwhelming hacking activity may incentivise industry and users to back away from the less secure devises.
INFLUENTIAL ACTORS Who can change the direction of the trend	It seems very difficult that anyone except by hackers could change the direction of this trend. If hacking activity becomes overwhelming for industry and users the trend may have to be painfully reversed.
EXPECTATION High/Medium/Low probability that the trend will develop fast and last for a long time	Very high expectation that the attacking surface area will continue to increase at a very fast pace.
ACTORS AFFECTED Who are the actors most influenced by the trend, and how are affected	All - Difficult to find any actor that will not be affected as digitalisation is ubiquitous
GEOGRAPHICAL SCOPE Local/National/International	International

ANALYSIS

	S&T system	Private organizations	Civil society	Government bodies
OPPORTUNITIES	Opportunity to double down on improving the privacy and security of their devises and services	Having better security systems than other similarly appealing companies may be enough to keep hackers away.	Opportunity to demand higher security standards and laws. Increased demand of cybersecurity specialists.	Opportunity to overcome opposition to mandating higher standards in privacy and security.
RISKS	Not being up to the challenge of producing secure by design devises and networks.	Prioritising growth over securing their multiplying points of attack.	More and more exposition to all kinds of cyber-attacks.	Being too slow producing the privacy and security standards needed for devises and networks to be secure by design.



TREND 2: RISE OF IOT EDGE COMPUTING

DESCRIPTION

The number of organisations that use IoT devices with on-board analytics capabilities, edge computing, is rising rapidly. Carrying out the computing as close as possible to the source of the data that's being analysed increases privacy as well as speed while reducing the amount of data transmitted to the cloud (relieving network congestion). This is enabled by ever smaller, powerful and energy efficient devises. Although privacy is increased by edge computing, it requires special encryption mechanisms —data must travel between distributed nodes— and the choice of security methods available to edge devises is limited —they are usually resource-constrained—. Limited losses by hacks due to devises holding only few data.

MANIFESTATION

SIGNALS How does the trend manifest, what are their signals?	On the one hand, the number of companies using edge computing is rapidly increasing. On the other, the expected explosion of IoT use and AI development will push its adoption and capabilities much further.
AREA	IoT
SUBAREA	Edge computing
NATURE OF THE TREND	Technologic
IMPACT High/Medium/Low	High impact to the networks by decreasing data transfer. Medium impact to companies by reducing costs and increasing efficiency Medium impact on privacy and security.
LEVEL OF DEVELOPMENT Weakly developed/ Moderately developed/ Fully developed	Moderately developed – Edge computing origins date back to the late 1990s, with the first commercial services in early 2000s. However, edge computing, the cloud and the IoT reinforce each other. Therefore, advances in the latter (particularly with wide adoption of 5G) coupled with advances in AI will greatly spur further development of edge computing.
FACTORS Aspects that may affect the development of the trend	The development and adoption of AI and IoT will affect the adoption of edge computing. The long waited deployment of 5G will indeed help in this regard.
INFLUENTIAL ACTORS Who can change the direction of the trend	Hardware providers, cloud/IoT vendors and software companies, as well as AI developers. In addition network providers and governments (by adopting and spreading 5G and further broadband technologies).
EXPECTATION High/Medium/Low probability that the trend will develop fast and last for a long time	High expectation that the trend will develop fast and last for a long time unless cyber-attacks become so prevalent that prevent it.
ACTORS AFFECTED Who are the actors most influenced by the trend, and how are affected	Industry: companies using IoT or cloud computing can enjoy more efficient, fast and private architectures that take less bandwidth to operate. Users: user of cloud services can enjoy faster and more private services. Networks: need to hold less traffic of data.
GEOGRAPHICAL SCOPE Local/National/International	International

ANALYSIS

	S&T system	Private organizations	Civil society	Government bodies
OPPORTUNITIES	Opportunity to develop further edge computer technology and monetise it	Decreased connectivity costs, increased efficiency, and decreased losses by potential hacks.	Enjoy faster and more private cloud services.	Safer and more private smart cities and smart administrations with lower costs.
RISKS	Focussing on fast innovation to meet demand may hinder the embedded security of the devises.	Same risks associated to the wide adoption IoT and cloud services: ever larger attack surface to protect from cyber-attacks	Larger exposure to cyber-attacks.	Not mandating the appropriate level of security could either leave users exposed or hinder the adoption of edge computing.

Source: Popper et al. (2022)

TOP 12 POSITIVE TRENDS

Trends in Artificial Intelligence Research

AI cybersecurity use increasing (macrotrend).

Edge computing enhances privacy, speed, reduces data transmission.

Data privacy prioritised, compliance pressures increase talent demand.

Multi-factor authentication ubiquitous, specialised apps improve access security.

Trusted networks shift to identity-based authentication, zero trust model.

Companies invest in security culture, combat social engineering risks.

Cybersecurity convergence simplifies, creates single points of failure.

Cyberinsurers monitor networks, adjust coverage based on risk exposure.

Infrastructure gap widens, empowering companies in AI development.

Paradigm shift reshapes government and firm roles in digital geopolitics.

Compute supply chain gains regulatory importance in AI development.

AI's significance alters semiconductor dynamics, future efficiency improvements expected.

Source: Popper et al. (2022)

TOP 10 NEGATIVE TRENDS

Trends in Artificial Intelligence Research

Expanded attack surface enables non-PC-based hacking.	AI exploits vulnerabilities, improving performance.	Smarter supply chains vulnerable to cyberattacks.	Sophisticated social engineering bypasses cybersecurity advancements.	Demand for cybersecurity experts exceeds talent supply.
Transition to AGI poses significant dangers.	Ransomware attacks increase, targeting vulnerable victims.	Hacktivism rises, driven by geopolitical events, collective targeting.	Business leaders acknowledge cybersecurity but lack prioritisation.	AI exploits socio-technical systems, unprepared for scale and speed.

Source: Popper et al. (2022)

ENABLING & HINDERING DEVELOPMENTS

Trends in Artificial Intelligence Research

1. Quantum Computing
2. Edge Computing
3. Neuromorphic Computing
4. Federated Learning
5. Generative Adversarial Networks (GANs)
6. Explainable AI (XAI)
7. Transfer Learning
8. Natural Language Processing (NLP)
9. Reinforcement Learning
10. Data Privacy and Security Tools

1. Adversarial Attacks
2. Data Bias and Discrimination
3. Lack of Interoperability
4. Ethical Considerations
5. Limited Explainability
6. Regulatory and Legal Frameworks
7. Scalability and Efficiency
8. Data Accessibility and Quality
9. Computational Power & Resource Needs
10. Algorithmic Transparency and Interpretability

Source: Popper et al. (2022) + ChatGPT

SMART Foresight

Fully-Fledged Process

SMART

SCOPING

Defining the rationales, objectives, budget, duration, time horizon, coverage and the methodology.

MOBILISING

Defining the sponsors, research/support teams, target groups, methodology and domain experts, champions and outreach.

ANTICIPATING

Combining outward-looking, inward-looking and forward-looking approaches to anticipate possible futures.

RECOMMENDING

Developing sound and robust advice based on multiple stakeholders' insights and needs of the implementation space.

TRANSFORMING

Assessing and managing the foresight process so as to achieve its objectives and facilitate the implementation of relevant actions.

SMART Foresight is a systematic, participatory, prospective and policy-oriented process aimed to actively engage key stakeholders into a wide range of activities anticipating, recommending and transforming (ART) technological, economic, environmental, political, social and ethical (TEEPSE) futures.

OPPORTUNITIES vs RISKS

Trends in Artificial Intelligence Research

1. Threat detection and prevention
2. Automated incident response
3. Intelligent threat hunting
4. Behaviour-based authentication
5. Intelligent vulnerability management
6. Secure software development
7. Malware detection and analysis
8. Real-time threat intelligence
9. Privacy-preserving analytics
10. Cybersecurity workforce augmentation

1. Adversarial attacks
2. Data privacy and protection
3. Bias and fairness
4. Explainability and interpretability
5. Malicious use of AI
6. Data integrity and authenticity
7. Scalability and efficiency
8. Insider threats and model poisoning
9. Lack of skilled cybersecurity professionals
10. International collaboration and standards

Source: Popper et al. (2022) + ChatGPT

SMARTEST Foresight

Fully Fledged & Continuous Process

Engaging key players in the systematic mapping of Research and innovation needs and challenges for AI in cybersecurity

POSITIVE & NEGATIVE WILDCARDS

Trends in Artificial Intelligence Research

1. Medical breakthroughs
2. Sustainable energy solutions
3. Climate change mitigation
4. Enhanced transportation systems
5. Increased productivity & economic growth
6. Personalised education
7. Cybersecurity advancements
8. Efficient resource management
9. Enhanced creativity and innovation
10. Improved accessibility and inclusion

1. Unintended system behaviour
2. Autonomous weapons and warfare
3. Job displacement & socioeconomic inequality
4. Manipulation and misinformation
5. Privacy breaches and surveillance
6. Bias and discrimination amplification
7. Dependence on AI systems
8. Ethical dilemmas and accountability gaps
9. Socio-cultural disruption
10. AGI runaway scenario

Source: Popper et al. (2022) + ChatGPT

RESEARCH AGENDA

Trends in Artificial Intelligence Research

Research Agenda

1. ML for evolving cyber threat detection
2. AI automation for incident response
3. Intelligent threat hunting and proactive identification
4. AI-enhanced user authentication and fraud detection
5. ML and predictive analytics for vulnerability assessment
6. AI-based software vulnerability prevention
7. Improved malware detection with AI algorithms
8. Actionable insights from diverse threat data using AI
9. Privacy-preserving analysis for secure collaboration
10. AI automation for augmented cybersecurity teams

Source: Popper et al. (2022) + ChatGPT

INNOVATION AGENDA

Trends in Artificial Intelligence Research

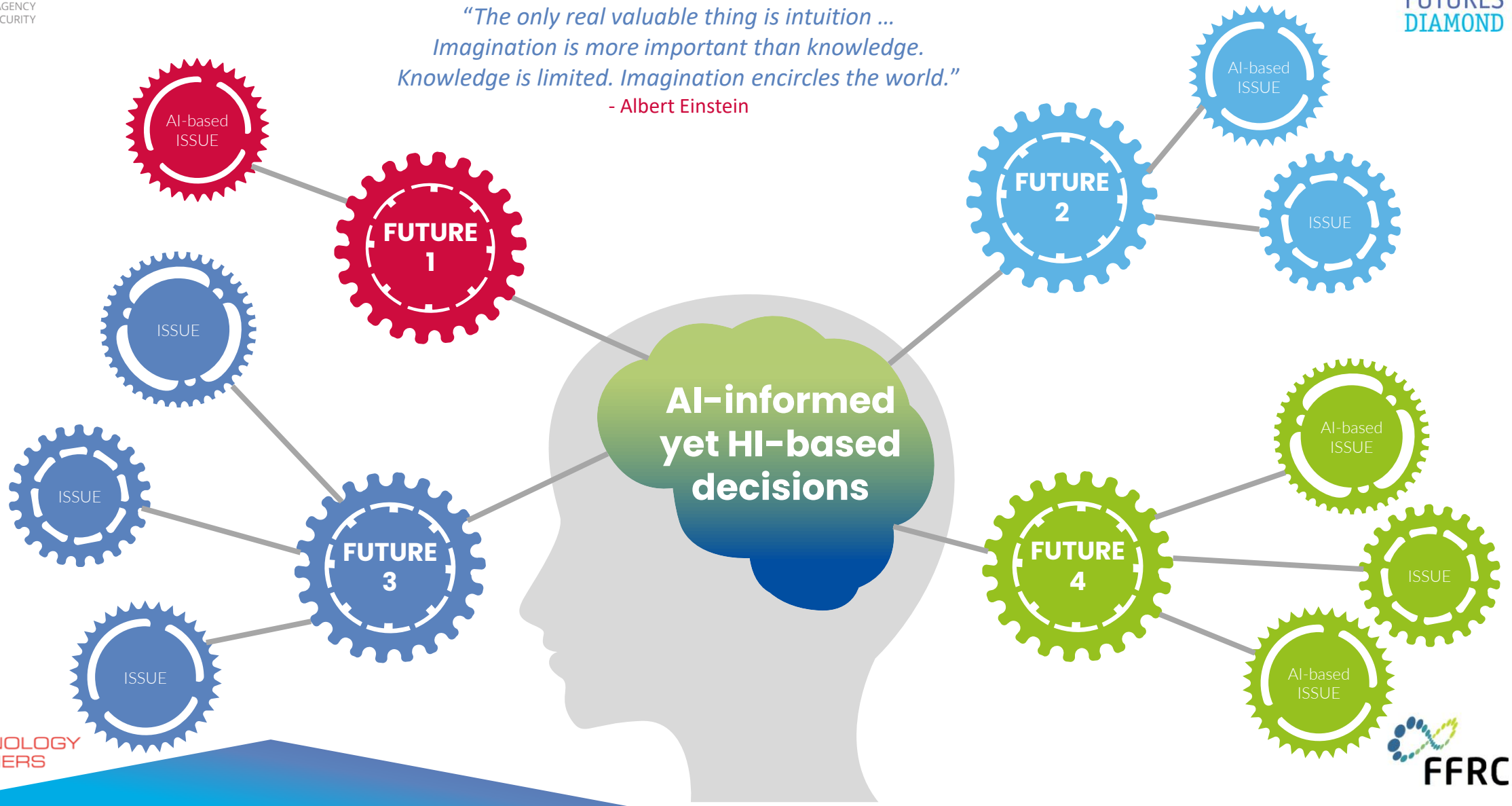
Innovation Agenda

1. AI-enabled proactive threat identification and mitigation
2. AI-powered incident response automation
3. Efficient threat hunting and investigation with AI analytics
4. Adaptive authentication with AI-based continuous monitoring
5. AI-driven vulnerability management automation
6. Secure coding enhanced with AI-based tools
7. AI-based detection of known and unknown malware
8. Real-time threat intelligence with AI platforms
9. Privacy-compliant advanced analytics using AI
10. Cybersecurity collaboration fostered by AI-powered platforms

Source: Popper et al. (2022) + ChatGPT

Human Intelligence (HI) at the Core

"The only real valuable thing is intuition …
Imagination is more important than knowledge.
Knowledge is limited. Imagination encircles the world."
- Albert Einstein



TECHNOLOGY PARTNERS

Key Takeaways

Trends in Artificial Intelligence Research

Takeaway 1	Takeaway 2	Takeaway 3	Takeaway 4	Takeaway 5
AI presents immense opportunities for cybersecurity	AI-driven risks demand attention and weak signals analysis	Collaboration and interaction are key for R&I agenda co0creation	Strive for explainability, transparency and evidence-based knowledge	Human expertise and creativity remain vital

Source: Popper et al. (2022) + ChatGPT

ENISA
AI CYBERSECURITY CONFERENCE

7 June, Brussels

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

REGISTER TODAY TO JOIN ME

Rafael Popper

Director of Futures Diamond (UK) and Adjunct Professor at Finland Futures Research Centre (FFRC) of the University of Turku (FI)

THANK YOU

FUTURES DIAMOND

FFRC