Security Conference

ENISA WORK ON CYBERSECURITY R&I NEEDS & PRIORITIES FOR AI, & WHAT IT MEANS FOR STANDARDIZATION"

Presented by: Corina Pascu

CYBERSECURITY RESEARCH IS A KEY PRIORITY FOCUS FOR THE EU

ENISA…

contributes to the EU Strategic Research Agenda in the field of cybersecurity (Art. 11 of the Cybersecurity Act)

advises the European Cybersecurity Competence Centre (ECCC) defining a strategic agenda and a work programme

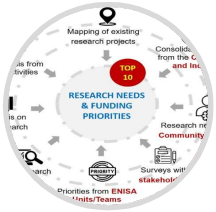
supports the implementation across EU Member States and maintain discussions with the key stakeholders and the research community

ENISA AND CYBER RESEARCH – A JOURNEY

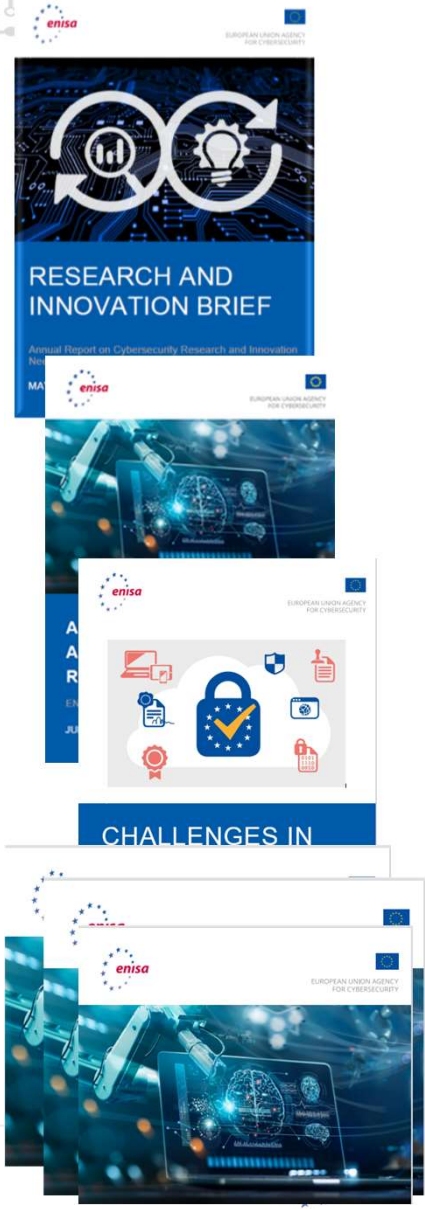
2021 Research needs & priorities

1. The age of intelligent systems (AI)
2. Computational security
3. Cybersecurity in life sciences (cyberbiosecurity)
4. Interdisciplinary in the research of core fields (AI in cryptography, next-gen communications etc)

2022 "Zooming in" on AI – areas of focus



What's going on in 2023



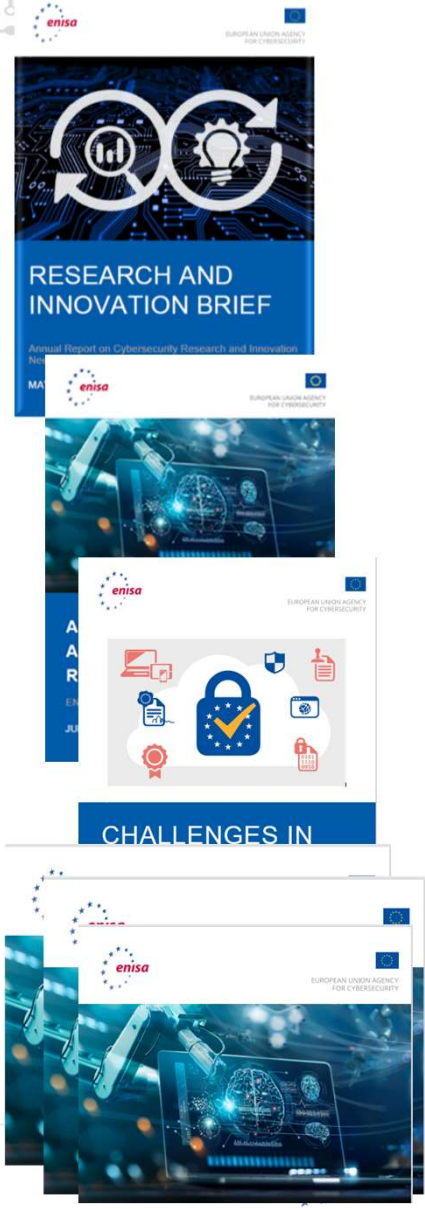
ENISA AND CYBER RESEARCH – A JOURNEY

2021 Research needs & priorities

2022 “Zooming in” on AI – areas of focus

1. AI and cybersecurity (securing AI and AI for cybersecurity): current state-of-play, future trends, gaps
2. The potential role of AI in cyber risk/ cyber insurance
3. The potential role of AI in cyber defence (SOCs)

What’s going on in 2023



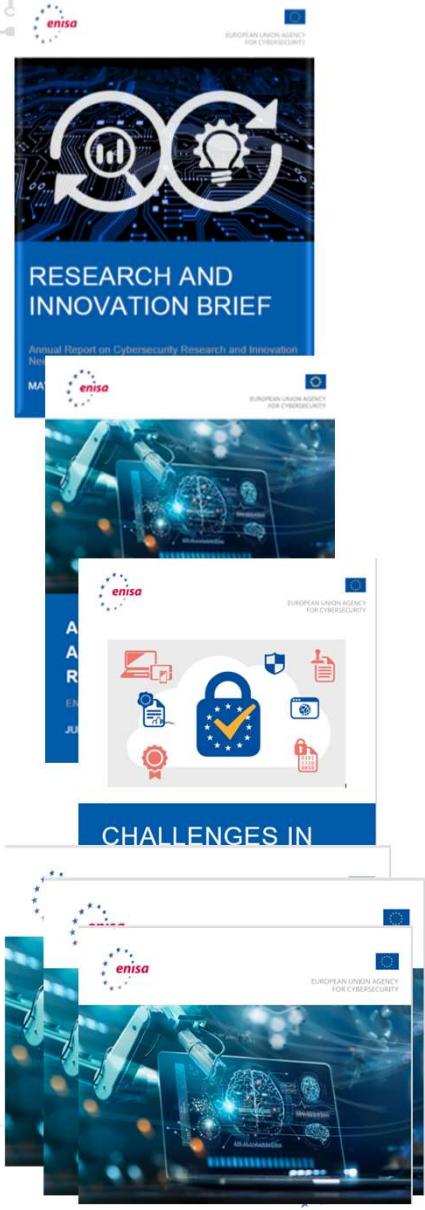
ENISA AND CYBER RESEARCH – A JOURNEY

2021 Research needs & priorities

2022 "Zooming in" on AI – areas of focus

What's going on in 2023

1. R&I Roadmap - the areas likely to impact the digital single market in the next 5 years
2. CyberRIO (Cyber R&I Observatory) incl. a Foresight exercise in R&I
3. Support to ECCC



CYBERSECURITY AND AI R&I ARE WE (EUROPE) READY?

Diversity	• Spread **geographically** and **topically** from basic research to prototyping and AI-aaS, specialised or generic;
Specialisation	• **Variety of focus areas**, incl. critical infrastructures, automated vehicles, IoT security, cryptography, healthcare, finance, cyberdefence, terrorism, smart cities, industry 4.0, and public sector
Critical infrastructures and IoT	• EU projects: reinforcing IoT cybersecurity, often with the help of AI, in domains such as **industry, health, smart cities** and **public sector**
Trust-oriented explainability/ shareability	• incl. **privacy protection**, law enforcement and regulatory governance issues • Making AI **more accessible, understandable, verifyable and usable**: promoting in practice the adoption of AI–aaS;
Ethics/privacy	• protection of human rights, e.g. through data anonymisation, and ensuring **human oversight** through situational awareness and inclusion in decision-making;

CYBERSECURITY RESEARCH TRENDS – LOOKING OVER THE HORIZON

Technological

- Advanced computing (next-gen microprocessors, edge and fog computing, HPC, QC) and ubiquitous computing (next-gen IoT, CPS)
- AI-everywhere (new! LLMs)
- Next-gen communications
- Space technologies
- Metaverse
- Internet of Senses
- System of systems (how to manage cybersecurity threats and risks and achieve cyber resilience)

CYBERSECURITY RESEARCH TRENDS – LOOKING OVER THE HORIZON

Non-technological

- Digital sovereignty and the related cybersecurity conditions underpinning it
- Privacy and ethics
- Supply chain security, quantum-ready security
- The porous continuum between fake news and disinformation, cybercrime, cyber and hybrid wars (the importance of Advanced persistent threats (APTs) e.g. relations with non-democratic countries and hackers' manoeuverings , Pegasus spyware, but also the Nord Stream and other war-related mysteries…)
- Critical infrastructures as key stake in the context of hybrid wars and attacks
- International cooperation e.g. global harmonization of cybersecurity

AI HAS TRANSFORMATIVE POTENTIAL IN CYBER INSURANCE

AI use abounds across the Insurance Value Chain (IVC)

Eling et al. (2021)

EIOPA (2021)

Advanced statistical techniques from AI/ML

potential for wider use in cyber risk modelling and cyber insurance

among other methods;

(X)AI in cyberinsurance e.g.

Systematic review "Explainable Artificial Intelligence (XAI) in Insurance"

https://doi.org/10.3390/risks10120230

GenAI

attackers leveraging GenAI today e.g. attacks orchestration

BUT also opportunities for genAI for security risk management.

AI HAS TRANSFORMATIVE POTENTIAL IN CYBER INSURANCE BUT …MAJOR OBSTACLES

CHALLENGES

- **Sourcing data to train AI** and ML models is a key challenge that insurers will need to overcome. (lack of) Data availability and data quality are important factors. They may hinder the use of advanced statistical methods and ML/AI in cyber risk modeling ;
- Domain-specific **definition of explainable AI models** (XAI) relevant to insurance practices;
- Bias in AI models could potentially lead to **discriminatory behaviour of the AI** system
- **Methods must be explainable** and fair/unbiased in order to provide validated benefits (and not additional risks). (Human and algorithmic) bias inherent to black-box AI systems threatens trust within the insurance industry;

For more details see the forthcoming report 'Weber, S, Scherer, M., Challenges in Cyber Risk and Cyber Insurance: Models, Methods and Data', editors: Corina Pascu (ENISA) and Marco Barros Lourenco (ENISA), forthcoming 2023.

AI IS A KEY ENABLER TO IMPROVE EFFECTIVENESS OF SOC OPERATIONS

KEY FINDINGS

- Innovation in cybersecurity software for SOCs is mainly **driven by the private sector**.
- **Access to cybersecurity data for research** purposes continues to be a **critical constrain**.
- **CTI sharing** continues to be an important element of SOCs operations.
- **AI is key enabler** to improve the efficiency and effectiveness of SOCs
  - training system to analyse data extract relevant indicators;
  - recognising malicious behaviour in encrypted network traffic;
  - extracting relevant information from unstructured data;
  - supporting analysts with suggestions from historic data;
  - automating detection in digital forensic data;
  - improving the risk assessment of vulnerabilities;
  - analysing data for improving asset management and dependencie

AI IS A KEY ENABLER TO IMPROVE EFFECTIVENESS OF SOC OPERATIONS

KEY FINDINGS

ENISA R&I Brief on Artificial Intelligence in Cyber Defence

- Security Operations Centres SOCs
- forthcoming 2023

18 specific recommendations cyber research on AI for cyber defence (SOCs) grouped into five categories

1. Cyber Threat Intelligence
2. Information Security Event Management
3. Incident Management
4. Vulnerability Management
5. Preventive Security Controls.

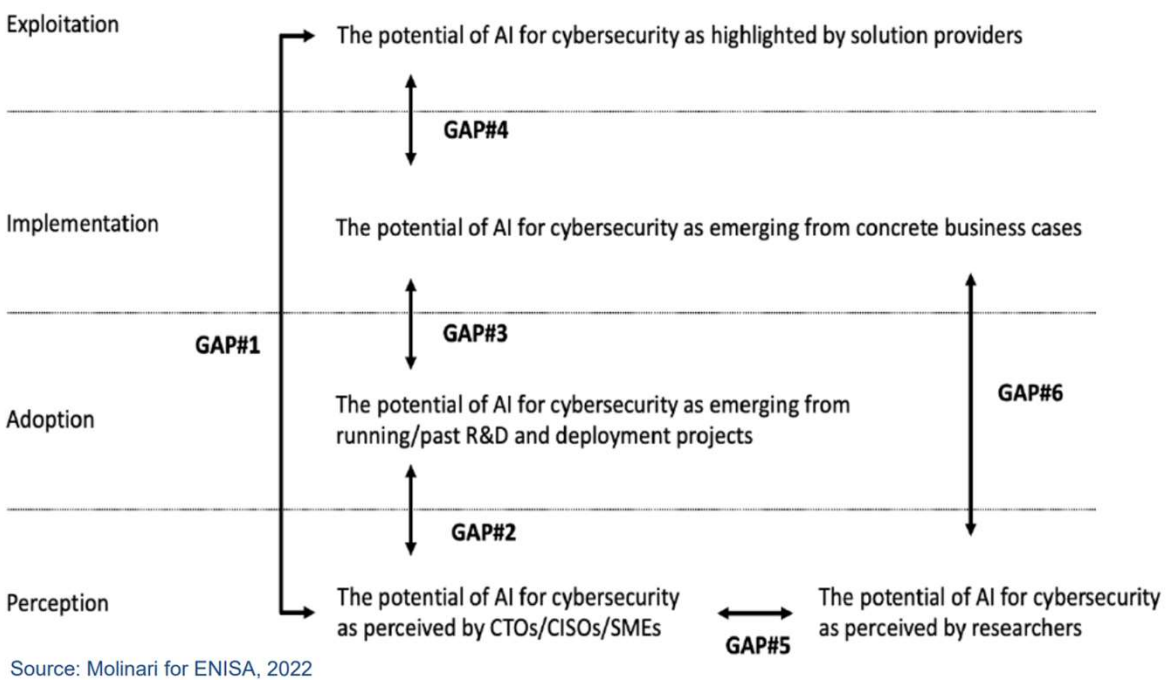
A GAP ANALYSIS

Lack of adequate information regarding the potential of AI solutions for Cybersecurity (because of the experimental nature of most AI solutions?)

Too few demonstration activities with convincing business cases for the value of AI solutions for Cybersecurity

Perception gap between research and business community: hinders efforts to match the design of R&D projects with market solutions

Limited capacity of R&I projects to solve existing or potentially problems associated with business-driven application domains



Source: Molinari for ENISA, 2022

QUO VADIS CYBER RESEARCH AGENDA AND AI

Data , data, data…
…and open access

Leveraging AI for cybersecurity research

Promote AI interpretability and explainability through e.g.

- funded deployment actions
- introduction of standards
- certification models

And more…

ENISA Roadmap (2023)

CYBER RESEARCH IN RELATION TO STANDARDIZATION ACTIVITIES IN AI

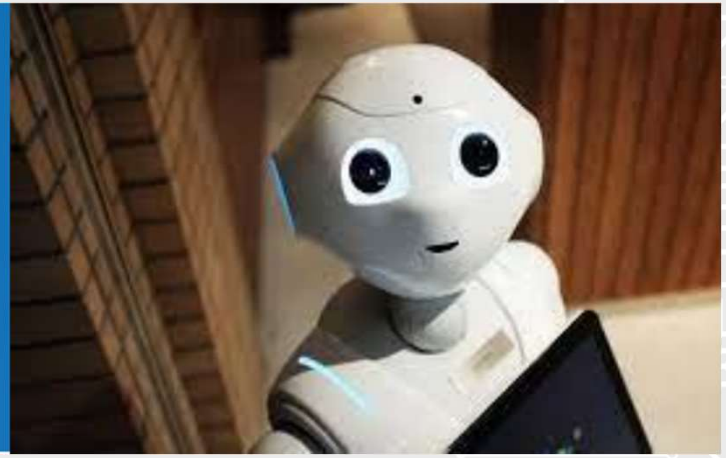
SOME KEY FINDINGS

- Standards and regulations can **shape innovation** and wider adoption e.g. quality standards reduce the risks associated with new technologies and level the playing field and therefore promoting competition (and so innovation);
- Domains covered by standards are **expanding** (e.g. Artificial Intelligence and Big Data); standards also important at the adoption and diffusion stage UKRI(2022)
- **Standardizing data across systems is the key** to reliably reproduce and compare existing AI-based solutions;
- Support for research activities to assess how AI that can be transferred into standards for certification of products, processes and services involving AI;
- Development of a standardised framework considering diverse malicious attempts, cases, security-by-design is a key challenge;

ENISA Research and Innovation Annual Brief (2023) and ENISA Roadmap (2023) and own's elaboration

THANK YOU FOR YOUR ATTENTION

Watch out
what's next...



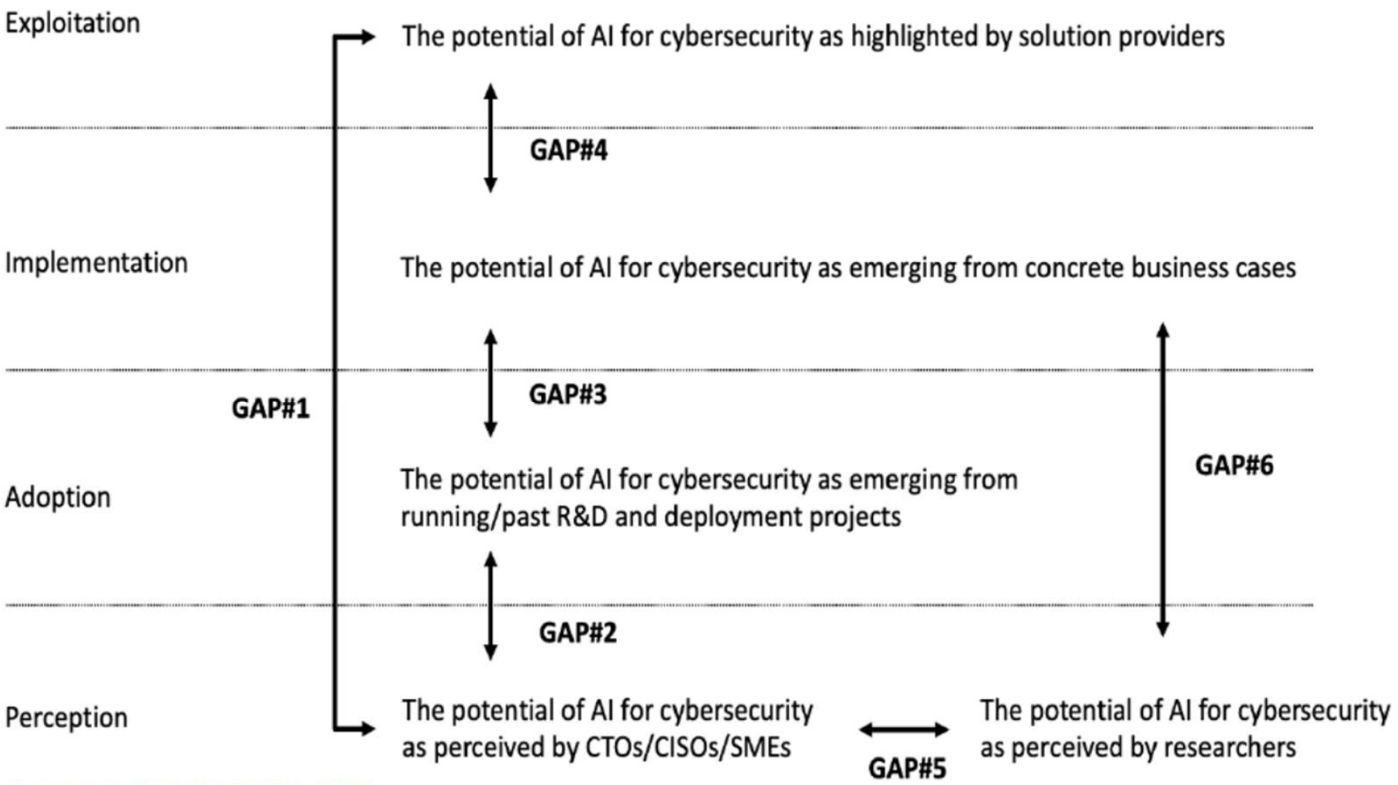
Agamemnonos 14, Chalandri 15231
Attiki, Greece

ETSI Security Conference 2023 - ENISA on AI R&I and Standards - Corina Pascu

corina.pascu@enisa.europa.eu

www.enisa.europa.eu

GAP ANALYSIS



Source: Molinari for ENISA, 2022