EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AN UPDATE ON ENISA' WORK ON CYBERSECURITY RESEARCH.

EMERGING TRENDS AND CHALLENGES

Corina Pascu
Cybersecurity expert

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)
- ENISA 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

CYBERSECURITY AND AI R&I: “NO FREE LUNCH”

ARE WE (EUROPE) READY?

- **Diversity**: Topical (from basic research to prototyping and AI-aaS, specialised or generic) and geographical spread;
- **Specialisation**: high variety of focus areas, including critical infrastructures, automated vehicles, IoT security, cryptography, healthcare, finance, cyberdefence, terrorism, smart cities, industry 4.0, and public sector
- **Critical infrastructures and IoT**: several EU projects are working on different ways to reinforce IoT cybersecurity, often with the help of AI, in domains such as: industry, health, smart cities and public sector
- **Trust-oriented explainability/shareability research** (incl. privacy protection, law enforcement and regulatory governance issues). Making AI more accessible, understandable, verifiyable and easily usable: promoting in practice the adoption of AI–aaS;
- **Ethics/privacy** e.g. 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)

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' manoeuvrings , 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

OPPORTUNITIES

- Smart cities as Systems-of-systems (SoS): the convergence and integration of multiple systems and technologies, powered by AI, will analyse large data sets to provide services to citizens;
- IoT aided smart city services – IoT holds potential for transformative change, but also significant impact on privacy and cybersecurity. Novel use cases and applications expected in the next decade e.g. the Industrial Internet of Things (IIoT) with cloudification, Internet of Things Senses (IoTS) (holographic communication ,multisensory extensions such as ‘holoportation’)
- Security of IoT devices is a priority in industrial R&D e.g. main areas of research include the development of trustworthiness models for edge IoT, integration of edge computing and artificial intelligence (AI) in IoT systems. self-adapting systems based on a digital twin and AI-based technology, as well as virtualisation and simulation tools for managing the evaluation of edge IoT system dependability, among others
- Integration of edge computing and artificial intelligence (AI) in IoT systems.: AI can improve the performance, efficiency, and functionality of IoT systems e.g. anomaly detection, optimization, and automation.

EMERGING TRENDS IN IOT SECURITY RESEARCH – A TWO-SIDED COIN

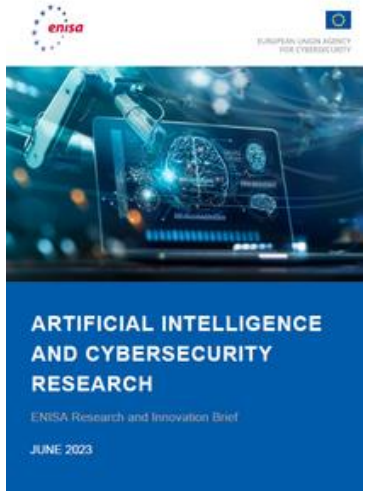
- IoT security research needs to address the security challenges and risks of edge computing and AI in IoT systems e.g. develop methods and tools to secure edge devices and the AI models (edge devices may have limited resources and capabilities to implement security measures, and be exposed to physical attacks; AI algorithms vulnerable to adversarial attacks)
- Built-in security features i.e. through blockchain support e.g. for secure and verifiable data sharing, identity management, access control
- But challenges e.g. scalability, performance, and interoperability issues, consume a lot of energy and resources.; legal, regulatory, and ethical questions, such as data ownership, governance, and compliance;
- Human factors and user experience are important for IoT security research;
- The convergence of multiple technologies increases the attack surface, threat exposure and systemic risk across the infrastructure

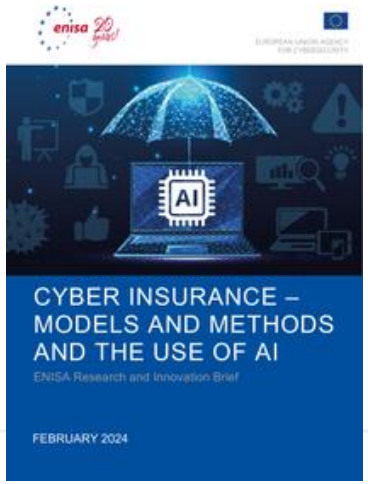
ENISA PUBLICATIONS AND RELEVANT WORK

ENISA report on Artificial Intelligence and Cybersecurity Research https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

ENISA report on Cyber Insurance - Models and methods and the use of AI https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai/@@download/fullReport

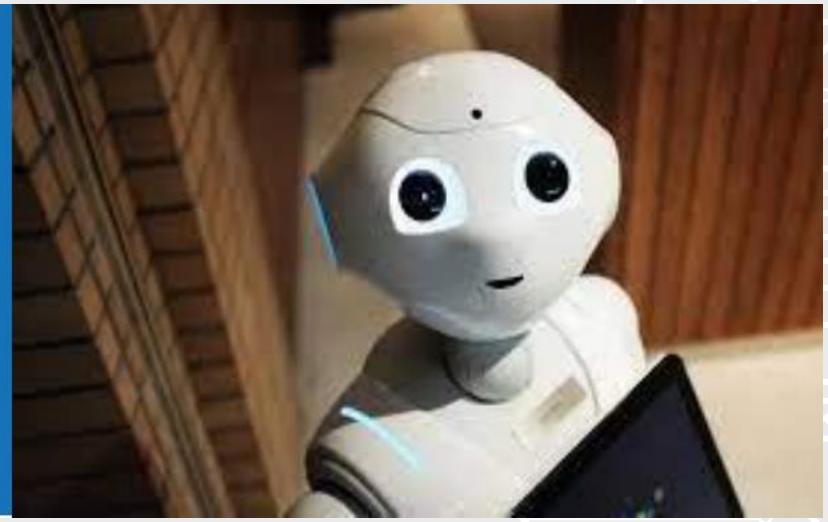
Further ENISA work used as internal baseline:
-on cybersecurity research and innovation roadmap across the EU
-research Topics on Cyberbiosecurity, Hardware Assisted Security, Cryptography Research, AI in Security Operations Centres (SOCs)
-Research and Innovation Brief
-State of Play and Future Trends in AI and cybersecurity research and innovation





THANK YOU FOR YOUR ATTENTION

Watch out
what's next...



Agamemnonos 14, Chalandri 15231
Attiki, Greece

(+30) 281 4409536

info@enisa.europa.eu

www.enisa.europa.eu