EUROPEAN UNION AGENCY
FOR CYBERSECURITY

AN UPDATE ON ENISA' WORK ON CYBERSECURITY RESEARCH AND INNOVATION NEEDS AND PRIORITIES

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

ENISA AND CYBER RESEARCH – A JOURNEY

Research needs and priorities - (4 themes in 2021)

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)

"Zooming in" on AI – areas of focus in 2022

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 in the store 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: “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

AI HAS TRANSFORMATIVE POTENTIAL IN CYBER INSURANCE

OPPORTUNITIES

- AI use abounds across the Insurance Value Chain (IVC) e.g. Eling et al. (2021) and EIOPA (2021)
- Advanced statistical techniques from AI/ML have the potential to be more widely used 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.

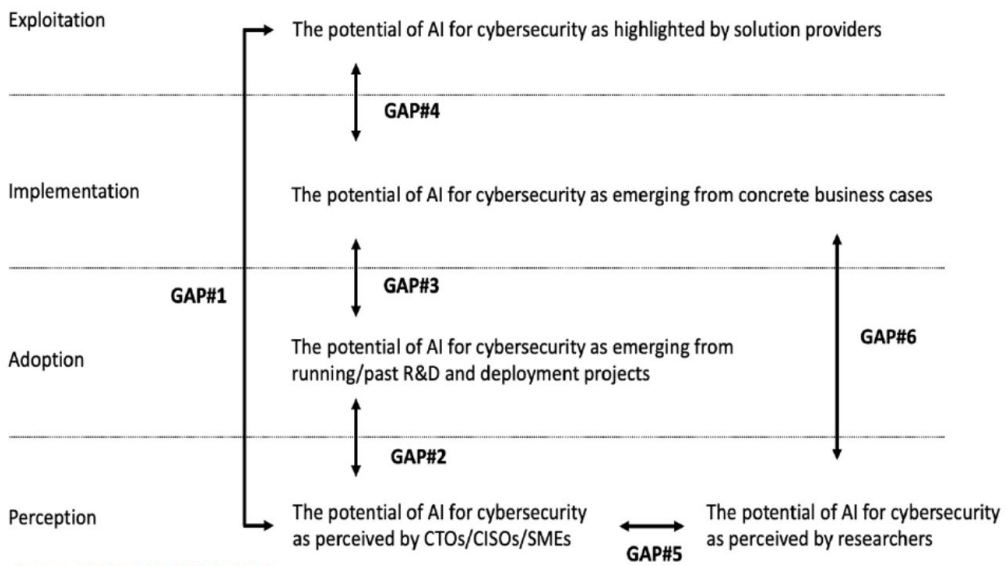
AI IS A KEY ENABLER TO IMPROVE EFFECTIVENESS OF SOC OPERATIONS

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.
- Cyber threat intelligence (CTI) sharing continues to be an important element of SOCs operations.
- AI is considered a key enabler to improve the efficiency and effectiveness of SOCs e.g. training system to analyse data in reports and extracting the relevant indicators and relations between them; recognising malicious behaviour in encrypted network traffic; extracting relevant information from unstructured data; supporting analysts with suggestions from historic data; automating the detection of attack traces in digital forensic data; improving the risk assessment of vulnerabilities; analysing data for improving asset management and dependencies
- ENISA R&I Brief on Artificial Intelligence in Cyber Defence (Security Operations Centres SOCs) forthcoming 2023 →18 specific recommendations, for cyber research on AI for cyber defence (SOCs) , grouped into five categories: Cyber Threat Intelligence, Information Security Event Management, Incident Management, Vulnerability Management and Preventive Security Controls.

A GAP ANALYSIS

- Lack of adequate information and knowledge regarding the potential of AI solutions for Cybersecurity, (or because of the experimental nature of most AI solutions
- Too few demonstration activities that can provide concrete/convincing business cases for the value and potential of AI solutions for Cybersecurity and be replicated. Only a minority of the prototypes/demonstrators actually have sound business cases;
- A perception gap between the researcher and the business community which hinders the efforts to match the design of R&D projects with market solutions;
- Limited capacity of R&I projects to solve existing or potentially emerging 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 appropriate initiatives (e.g. funded deployment actions, introduction of standards and certification models)
- And more…

ECCC IN PRACTICE

- bringing together stakeholders through public private partnerships and cooperation. E.g. funding initiatives aiming to establish a network of regional PPPs focused on cybersecurity innovation;
- catalysing innovation impacts from EU-funded research activities e.g. by including innovation impact as a post-project requirement in future EU fundings calls;
- generating new business opportunities especially for start-ups and SMEs e.g. developing a catalogue of cybersecurity technologies and services;
- improving knowledge transfer and development of entrepreneurial skills. E.g. inclusion of entrepreneurship and business culture as a subject in higher-education programmes;
- providing access to technical infrastructure for the development of cybersecurity products and services. E.g. dedicated/specific programme aiming to connect cybersecurity innovation hubs (EDIH) to clusters hosting technical infrastructures;
- fostering the creation of Cybersecurity Accelerators/Incubators. E.g. matchmaking (bringing together founders, business mentors and innovators to support early-stage start-ups) (ECCC Access-2-Finance Matchmaking series);
- establishing a community of investors in cybersecurity e.g. establishing a Cybersecurity Investors Forum that plays an active role in attracting public and private investment (including crowd-sourcing) in EU cybersecurity start-ups.

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