Foundation Forum 2022

Assured AI and Data Ecosystems: Innovations, Standards and Cybersecurity

The Policy Context

November 2022

Dr Robert Wortham and Catriona Gray

Introduction

Artificial Intelligence (AI) undoubtedly offers huge opportunities for businesses, public authorities, and citizens. We are already witnessing major transformations, enabled by AI, in fields including infrastructure, business processes, consumer products, and public services. The development and deployment of AI techniques across sectors, however, brings significant challenges, including for cybersecurity. This comes at a time when cyber attacks are increasing in scale, cost and complexity, and the number of devices linked to the Internet of Things (IoT) continues to grow.

AI has been characterised as something of a **'double-edged sword' for cybersecurity** (Taddeo et al. 2020). On the one hand, AI techniques can be used to support and automate cybersecurity operations and controls. At the same time, however, the application of AI can also open many new avenues for attack and expose organisations to additional risks. This is particularly apparent in safety-critical domains such as health, transportation, manufacturing, and critical infrastructure.

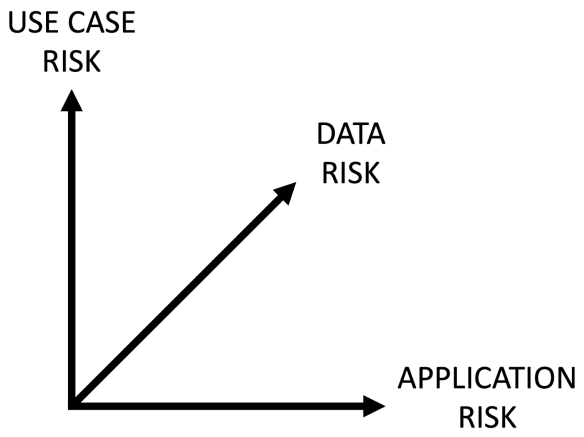
The European Union Agency for Cybersecurity (ENISA) divides this complex relationship between AI and cybersecurity into three key dimensions: **cybersecurity for AI, AI to support**

cybersecurity, and the malicious use of AI. The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) also addresses these three aspects of AI in its activities.

Cybersecurity for AI	This dimension concerns potential vulnerabilities and instances of insufficient robustness in AI systems. This includes, for example, the manipulation of data used in AI systems, data poisoning, adversarial model manipulation, attacks against cyber-physical systems, and integrity in the software supply chain.
AI to support cybersecurity	AI may be used as a tool to augment cybersecurity through the development of more effective controls. These might include automated cyber threat intelligence (CTI), smart forensics, email scanning, intelligent firewalls, and automated malware analysis. AI may also be used to support law enforcement agencies to detect and respond to cybersecurity related criminal activities.
Malicious use of AI	AI can be used maliciously by adversaries to create more sophisticated attacks. Examples of this include AI powered malware, social engineering, the creation of fake social media accounts, AI-augmented distributed denial of service (DDoS) attacks, deep fakes, and AI-supported password cracking.

Cybersecurity increasingly features in AI policy and standardisation instruments, including normative frameworks, regulations, and technical standards. At the same time, the importance of AI is recognised in cybersecurity instruments and agreements, such as the EU's Cyber Posture, approved in May 2022. However, as each of the three dimensions above suggest, **data is always a key vector of risk when it comes to using, securing and preventing the misuse of AI.** To understand AI and cybersecurity – and their relationships – we must look not only at AI and cybersecurity policy, but also at data policy, including the EU's data strategy and related legislation.

Applying a three dimensional risk-based approach



Use case risks - High-risk AI systems as defined in the EU AI Act
Data risks - Provisions of GDPR, Data Act and Data Governance Act
Application risks - The AI technology stack

EU cybersecurity policy initiatives

At the end of 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new **EU Cybersecurity Strategy.** The importance of cybersecurity for AI was explicitly addressed in the strategy:

"Cybersecurity must be integrated into all these digital investments, ***particularly key technologies like Artificial Intelligence (AI)****, encryption and quantum computing, using incentives, obligations and benchmarks."*

The strategy's measures include a review of the Directive on the security of network and information systems (NIS Directive) – the first piece of EU-wide legislation on cybersecurity. Since the NIS Directive was first adopted in 2016, the cybersecurity threat landscape has changed markedly, and in 2020 the Commission proposed a revision of the Directive. **NIS2 expands the scope of application** and strengthens the obligations of management bodies.

In September 2023, the Commission presented a proposal for a new **Cyber Resilience Act** which aims to protect consumers and businesses from products with inadequate security features. This is the first legislative instrument introducing EU-wide mandatory requirements for products with digital elements. The text of the

proposal also highlights the interplay of cybersecurity with other EU digital policies, including the proposed AI Act.

The European Commission has expressed its hope that the Cyber Resilience Act, like the AI Act, will strongly influence markets and standards-setting globally, with Lorena Boix Alonso, Director for Digital Society, Trust and Cybersecurity at DG CONNECT recently stating:

"This will impact not only the European Union. ***This will change the rules of the game globally, one way or another.*** *Because they will copy us or because they will not have the tools to abide by our rules. This is good not only for the level of cybersecurity but for the competitiveness of Europe."*

As well as these legislative initiatives from the European Commission, there are developments taking place in standardisation and certification. ENISA is currently examining the main considerations involved for developing a **cybersecurity certification scheme for AI systems,** and is expected to publish a report on its findings in the coming months.

Key questions

1. *Are cybersecurity solutions keeping pace with the growing use of AI and expanding digital and data supply chains?*

2. *What's the place of certification systems in building trust and confidence in these cybersecurity solutions?*

EU AI policy initiatives

The proposed European Union AI Act recognises the crucial role of effective cybersecurity in achieving the objectives of the regulation, including increasing the uptake of trustworthy AI. This is evident in the relevant cybersecurity provisions within the proposed Act. Recitals 48-51 highlight, amongst other things, the fundamental importance of technical robustness: high-risk AI systems should be ***"resilient against risks connected to the limitations of the system (e.g. errors, faults, inconsistencies, unexpected situations)*** *as well as against malicious actions that may compromise the security of the AI system* […]."

The Act recognises that **AI-specific assets**, such as training datasets or models, can be leveraged to attack either the AI

system or its underlying ICT infrastructure. As required by Article 9, these cybersecurity related risks will form part of the risk management systems that those responsible under the Act must implement.

The main cybersecurity-specific obligations of the Act are set out in **Article 15**, with corresponding transparency obligations in Article 13. The Act requires that high-risk AI systems have **appropriate levels of robustness, accuracy and cybersecurity** which must be maintained throughout the entire lifecycle. The exact technical solutions to be employed will depend on the circumstances and risks. These requirements overlap with existing legislation, namely the certification process as set out in Regulation 2019/881 on the European Union Agency for Cybersecurity and on information and communication technology cybersecurity certification (**'Cybersecurity Act'**), and indeed Article 42 of the AI Act explicitly refers to the Cybersecurity Act. It provides that high-risk AI systems which have already been certified or had a relevant statement of conformity issued under an existing cybersecurity scheme shall be **presumed to be in compliance** with Article 15.

The Commission has also recently presented the **AI Liability Directive** which lays down uniform rules for non-contractual liability for damages, including those associated with a breach of privacy obligations.

Key questions

1. *Most AI solutions involve complex value chains of partners and third-party suppliers. How will governance work throughout these value chains?*

2. *How will providers have confidence in the compliance of their sub-contractors?*

3. *Are compliance solutions already being developed?*

4. *How will this affect the power dynamics, especially between SMEs and multinationals?*

EU data policy initiatives

As part of its efforts to create a single market for data and to promote data-driven innovation, the European Commission has proposed several instruments. The **Data Governance Act (DGA)** creates a framework for data sharing by strengthening mechanisms to both increase data availability and overcome

obstacles to the reuse of data. Unlike GDPR, it is not solely concerned with personal data. Under the Act, data intermediaries are required to meet **licence conditions** designed to ensure their independence and restrict their re-use of data and metadata.

The proposed **Data Act** complements the DGA, and aims to increase the availability and interoperability of non-personal data. Although it is wide-ranging and sector-neutral, it will have particular significance for manufacturers of consumer electronics and specialised machinery, and cloud services providers. Whereas the DGA is an attempt to create a legal framework and processes to promote data sharing, the Data Act primarily focuses on clarifying which entities can create value from data, and under what conditions. Since 2018, **the value of the data economy** in the EU27 has increased from €301 billion to **€829 billion.**

Key questions

1. *How can the value-add of innovation using AI be accelerated?*
2. *What will be the impact of impending regulation on this innovation?*
3. *How do we build the skills we need to take advantage of the AI innovation opportunity?*

The standards landscape

EU legislation relies heavily on harmonised standards for its implementation. Under the AI Act, manufacturers ('providers') are incentivised to follow standards because of the presumption of conformity established in Article 40. European Standardisation Organisations (ESOs) – **CEN, CENELEC, and ETSI** – will be responsible for setting these standards following standardisation requests (SR) from the European Commission. The European standards regime also encompasses close cooperation and special agreements with ISO/IEC to ensure harmonisation, including mechanisms for the parallel approval of standards.

In 2019, CEN and CENELEC established the new CEN-CENELEC Joint Technical Committee (JTC) 21 Artificial Intelligence. **CEN-CLC/JTC 21 is responsible for the development and adoption of standards for AI** and related data and the provision of guidance to other Technical Committees concerned with AI. It identifies and adopts international standards already available, or under development, from other organisations like ISO/IEC JTC 1

and its subcommittees, namely SC 42 Artificial Intelligence. A similar committee, **CEN-CLC/JTC 13, is responsible for cybersecurity and data protection**.

ETSI has established an **Industry Specification Group on Securing Artificial Intelligence (ISG SAI)** which seeks to improve the security of AI through production of high-quality technical standards.

Key questions

1. *How will standards help Europe maximise the benefits and reduce the risks of AI?*
2. *How will standards help AI-driven innovation?*
3. *Are European standards bodies on track to deliver the right standards at the right time?*

Following the Foundation Forum 2022, we will be producing an outcome report with key reflections and findings based on the discussions we have today.

We welcome your input and interest.