




AI want(s) to break free: Can the EU secure the future of cyber?

AUTHORS: LÉA DORASCENZI, APOLLINE ROLLAND
EDITORS: PAULINE MASSART, GUILLAUME TISSIER

An aerial, high-angle photograph of a busy pedestrian crossing. The scene is filled with a diverse group of people walking in various directions. Long, dark shadows are cast across the asphalt, indicating a low sun position. The crossing is marked with wide white stripes. A circular manhole cover is visible in the center of the frame. The overall atmosphere is one of a bustling, active urban environment.

INTRODUCTION



At the time of writing, the European Union (EU) had finally reached an agreement to regulate AI¹, the final legal version of the AI Act being fine-tuned. Discussions have been raging over the pros and cons of the technology. From science fiction scenarios to the ChatGPT buzz, **AI is undoubtedly the technology of the moment. However, the real issue is not the technology itself, but rather what we choose to do with it.**

AI is complex and lies at the crossroads of numerous technologies. Seen by many as a potential threat, it also offers endless possibilities, with far-reaching impact for individuals, organisations and society as a whole. **Cybersecurity is no exception**, and questions abound as to the extent to which AI can improve cybersecurity or, on the contrary, spell its end. While AI can be used to strengthen the security of networks and information systems, it can also be weaponised for cyber attacks.

Countries around the world are trying to regulate the use of AI, recognising the difficulties in comprehending the full capabilities of this technology. The 2023 UK AI Safety Summit, where UK Prime Minister Sunak and US Vice President Harris announced the creation of AI Safety Institutes in their respective countries, was a major event in this area. With the AI Act², the EU intends to address the challenges posed by AI to ensure a secure future for Europe. As it did with the GDPR, the EU hopes its normative power will promote EU values in the development of AI, competing with global champions such as China or the United States. **The AI Act will therefore be the first major regulation to govern AI.** Will it meet safety expectations while continuing to promote innovation?



The challenge is to strike the delicate balance between leveraging the benefits of AI for cybersecurity and preserving the integrity of the digital space.

- 1 Timeline - Artificial intelligence, Council of the EU, URL.
- 2 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021, URL.

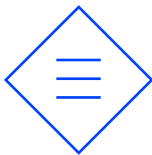
AI for cybersecurity, the promised land?

AI-BASED APPLICATIONS CAN IMPROVE
CYBERSECURITY, MORE SPECIFICALLY
PREVENTION, MITIGATION AND RECOVERY.



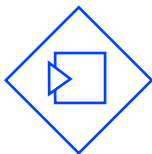
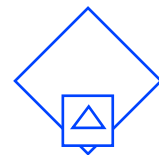
PREVENTION

In 2021, 34% of cyber incidents were linked to the exploitation of system vulnerabilities, a figure which continues to rise³. To tackle this, it is necessary to constantly monitor and update networks and IT devices to ensure that systems remain safe. AI is proving an effective tool to protect and make IT systems more robust. Numerous cybersecurity prevention applications using AI exist, including:



Planning and management support AI and machine learning techniques (ML) can perform simple tasks which support workflows and decision-making, for instance sorting and identifying assets such as IoT devices. It can also be used to plan and prepare for contingency in the event of an attack.

AI-based software testing helps to improve the robustness of algorithms by automatically analysing and testing systems. Using AI-powered behavioural analytics for instance, softwares can detect anomalies in system operations.



Automated penetration testing and AI-based fuzzing can be used to randomly and automatically flood IT systems with faulty or erroneous data, examine how the system reacts and, above all, proactively implement adjustments in the event of crashes or failures⁴.

AI-based vulnerability assessments: ML techniques (regression, classification, clustering) can be used to identify patterns in data or find correlations between large datasets automatically, quickly and repeatedly⁵.



By using AI to make IT systems more robust and resilient, organisations can save time and money and increase efficiency.

3 X-Force threat intelligence index, IBM 2023, [URL](#).

4 Artificial intelligence for cybersecurity: Literature review and future research directions, Kaur et al. 2023, [URL](#).

5 AI in cyber security: benefits and uses cases, Altamira 2023, [URL](#).

MITIGATION

In France, between 2020 and 2021, the number of cyber intrusions increased by 37%⁶. This increase is expected to continue on a global scale, especially as these attacks are generally not directed against a single device, but against a group of interconnected systems, some using cloud services. Almost one in two businesses in the EU uses cloud services, which exponentially increases the surface of attacks. This brings with it new requirements in terms of identifying, mitigating and responding to such attacks⁷. AI offers great potential for improving the mitigation of cyber attacks. It is an active field that already offers a number of solutions such as:

AI & HUMAN SYNERGIES

Associated to the work of human operators, AI makes security systems more adaptative and resilient. With a 24/7 operation and processing speed, AI can handle more data, respond quicker and avoid cognitive bias, by taking over repetitive and tedious tasks. Meanwhile, humans can focus on complex manual verifications, focus on interpreting data and concentrate on more strategic activities.



NEURAL NETWORKS AND ML FOR THREAT DETECTION TO IMPROVE SIGNATURE-BASED AND ANOMALY-BASED METHODS

Traditional signature-based detection relies on predefined attack patterns, while anomaly-based detection is limited by a finite dataset for defining "abnormal" behaviours. To overcome these limitations, the integration of ML with neural networks and deep learning (DL) offers a more advanced and adaptive approach, capable of learning complex patterns, adapting to new threats by adjusting their understanding of 'normal behaviour' over time, and processing large datasets.

AI-HONEYPOTS

Honeypots powered by AI can lure attackers away from critical data and valuable assets⁸. Once a threat is detected, AI-honeypots automatically redirect all internal and external attacks and collect, record and analyse attempted attacks to learn from them and strengthen system protection. Through behavioural analysis, AI-response techniques subsequently choose and recommend the best countermeasures⁹.

6 Une année 2021 marquée par la professionnalisation des acteurs malveillants, ANSSI 2022, [URL](#).
7 Cloud computing - statistics on the use by enterprises, Eurostat 2023, [URL](#).
8 Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution, Goosen et al. 2018, [URL](#).
9 Artificial intelligence for cybersecurity: Literature review and future research directions, Kaur et al. 2023, [URL](#).

RECOVERY

Recovery consists in restoring the affected entity's systems and operations after a cyber incident. The aim is to minimise the damage caused by the attack, reduce downtime and ensure business continuity, and involves activities such as eliminating malware, correcting vulnerabilities, restoring data from backups and implementing enhanced security measures to prevent future attacks. AI offers promising applications for this phase. For instance, it can **perform damage assessments, identify compromised systems or data and communicate results to operators**. ML techniques can be implemented to **automatically issue and scan through incident reports** in order to extract relevant knowledge from the attack, supporting operators to ensure data recovery and return to normal business activities¹⁰. AI-based incident response automation tools can **sort and analyse key takeaways from incident reports, proceed to routine checks and implement measures and processes to facilitate the work of SecOps teams**¹¹, formulating recommendations such as further encryption, the introduction of new security protocols or data sanitisation.

AI WANT(S) TO BREAK FREE - CAN THE EU SECURE THE FUTURE OF CYBER?

**While AI is a powerful cybersecurity tool,
it is not a silver bullet.**



**A holistic security strategy is a combination
of technology, human expertise and good practice.**

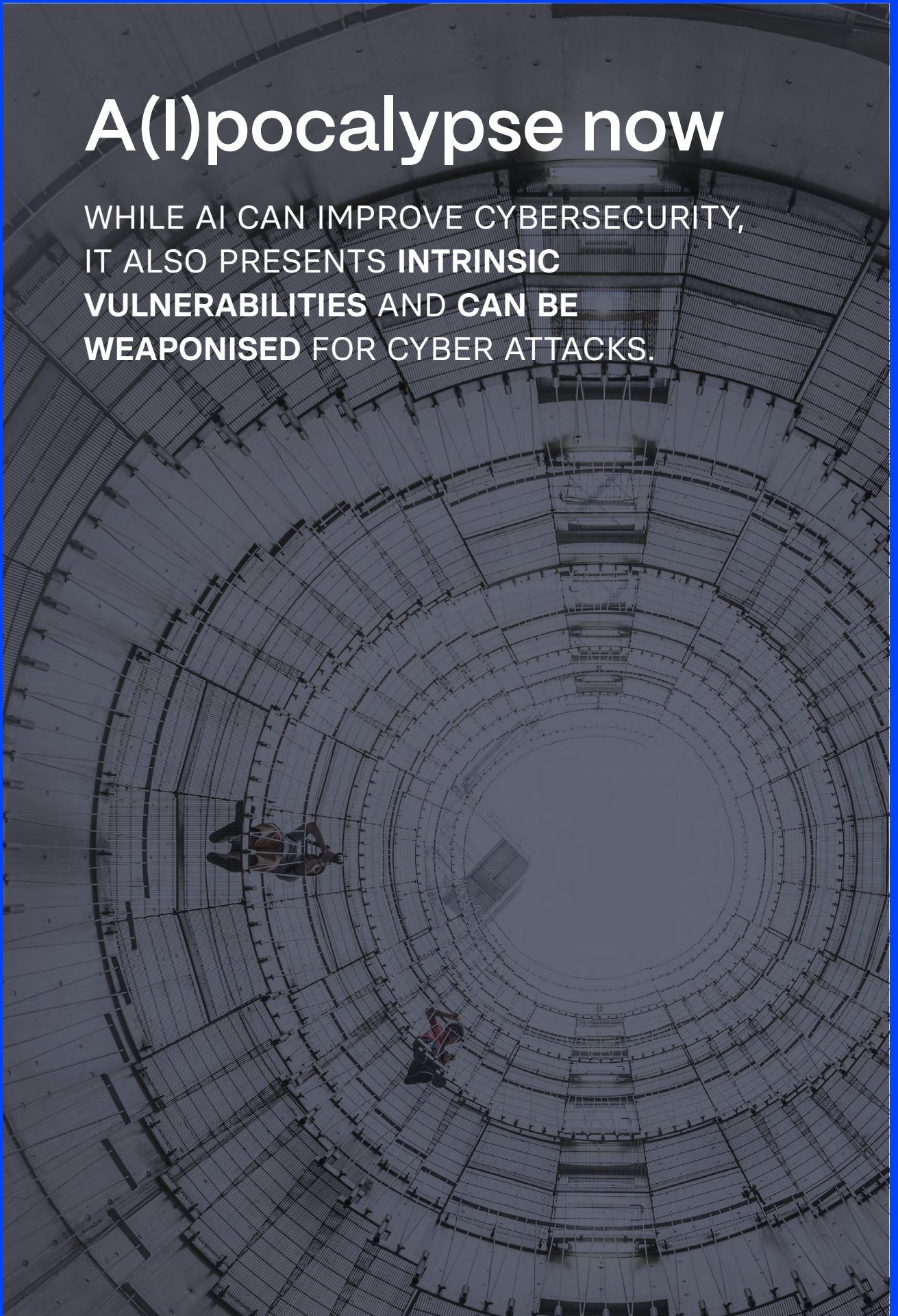


¹⁰ Artificial intelligence for cybersecurity: Literature review and future research directions, Kaur et al. 2023, [URL](#).

¹¹ Incident response automation: What it is and how it works, Irei and Froehlich 2023, [URL](#).

A(I)pocalypse now

WHILE AI CAN IMPROVE CYBERSECURITY,
IT ALSO PRESENTS **INTRINSIC
VULNERABILITIES AND CAN BE
WEAPONISED FOR CYBER ATTACKS.**



AI VULNERABILITIES

Understanding the **three basic approaches to AI** provides a starting point to identifying its **intrinsic vulnerabilities** for IT systems, namely **supervised, unsupervised and semi-supervised learning**. **Supervised learning** uses labelled dataset to predict outcome: each input example is associated with a corresponding output label. The algorithm is supervised and trained to classify data and predict outcomes accurately¹². With **unsupervised learning**, the algorithm analyses and clusters unlabelled datasets to discover hidden patterns or relationships without the need of human intervention¹³. At the crossroads of these two learning approaches is **semi-supervised learning** which uses training datasets with both labelled and unlabelled data. These different techniques each have their pros and cons, depending on the volume of data used, its quality and complexity¹⁴. Vulnerabilities can be encountered in all these different approaches and can **arise at any stage of the deployment of AI models**, i.e. during **training, testing** or **deployment phases**.

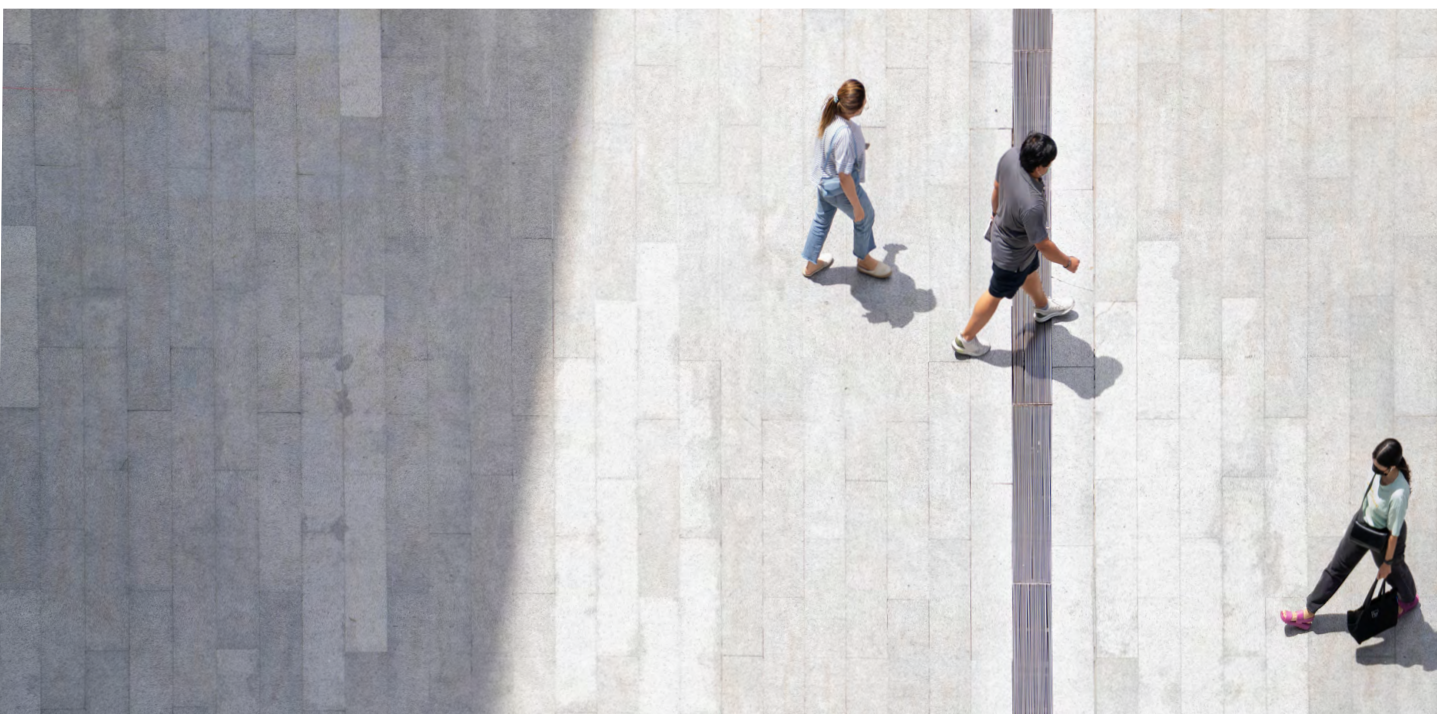
Understanding the AI threat landscape is essential for cybersecurity. This means understanding the entire lifecycle of the AI system, addressing security issues from data modelling through to algorithms. It is vital to identify all assets critical to the functionality of the system, including training data, model, ICT infrastructure, people, processes and physical infrastructure. In addition, a thorough analysis of potential threats and vulnerabilities, such as false positives, model manipulation or human error, is imperative.

*Source: Monika Adamczyk, ENISA
inCyber Agora event of the 20/11/2023.*

12 Supervised vs. Unsupervised Learning: What's the Difference?, IBM 2021, [URL](#).

13 *Ibid*

14 *Ibid*



The weak point of AI systems lies in their learning capacity. During the **training and testing phase**, the AI model evolves in a benign environment in which there is no adversary to contradict the model. In the case of supervised or semi-supervised learning, where the AI is trained to classify data and predict outcomes relying on training datasets, vulnerabilities emerge both from the modelling itself and from the input data:

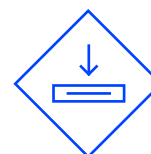


MODELLING ISSUES

If AI is not taught to categorise all possible future outcomes, the model will be inaccurate and produce errors. Adversaries could exploit such vulnerabilities by manipulating models, influencing their behaviours or by controlling a part of the training set outcomes¹⁵.

INPUT DATA ISSUES

AI is vulnerable to corrupted data inputs which result in inaccurate response from systems¹⁶. AI vulnerabilities come from the input data used in training and testing phases themselves, stages during which data and learning processes can be corrupted through **poisoning, evasion, misclassification, forgery** or **stealing of data**. If the training dataset is biased, insufficient, contains errors or noisy input, the model will make and repeat wrongful predictions¹⁷.



The **limits of perception and human intelligence** prevent operators from detecting and correcting these mistakes. Developers can make mistakes, fail to identify them and thus to mitigate their consequences¹⁸.

When deployed in the real world (i.e. non-benign environments), the **AI model will encounter many adversaries**. These may be malicious actors, but also simply situations or elements that the AI model did not face during training and testing, because that data was not present in the training datasets. To cope with such situations, the robustness of the AI model is crucial, i.e. the ability of an AI system to withstand a non-benign environment. A lack of robustness in the AI model will lead it to make wrongful predictions, produce errors, false positives and false negatives alike.

Finally, **the 'black-box nature' of AI, i.e.** the opacity and lack of transparency of AI systems, creates additional challenges as it prevents operators from truly knowing how the system operates¹⁹, whether there has been an attack or if the system operates as expected²⁰. This lack of transparency can lead to a lack of accountability, which calls for the development of AI models based on clear legal guidelines.

15 Artificial Intelligence and cybersecurity: opportunities and challenges, NSTC NITRD 2020, [URL](#).

16 *Ibid*

17 Artificial Intelligence and cybersecurity: European Union panorama, da Silva Costa 2021, [URL](#).

18 The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, Ansari et al. 2023, [URL](#).

19 Attacking artificial intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, Comiter 2019, [URL](#).

20 Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity, Taddeo 2019, [URL](#).

AI WEAPONISATION

The exponential increase in the number of cyber-threats has come with a diversification of types of attack: in 2022, 27% of attacks worldwide were extortion attacks, 21% backdoors and 17% ransomware. **AI is playing a major role in this increase and diversification.** The rapid democratisation of AI is enabling a growing number of malicious actors to weaponise it, while at the same time allowing an increasing diversification in the types of cyberattack. **AI expands existing types of cyber attacks** (extortion, malwares, poisoning, model or data disclosure, spam, etc.) **and even creates new forms of cyber threats** that humans would not be able to develop on their own (deep fakes, swarm attacks, breaking of CAPTCHAs, etc.²¹). AI is therefore used to reinforce the efficiency and effectiveness of current malwares and to develop new tools, skills and methods to conduct attacks. **AI makes cyber attacks faster, more discreet and capable of adapting to enhanced cyber defence measures.**²²

The **April 2018 cyberattack on TaskRabbit** is an example of an AI-assisted cyber attack. TaskRabbit, an online marketplace and services platform, fell victim to hackers who orchestrated a large Distributed Denial of Service (DDoS) attack using a botnet commanded by AI. The attack temporarily blocked the entire TaskRabbit site, and compromised users' personal information.

Source: IPV Network 27/06/2023.

Cyberattacks can target AI models themselves. They can occur during all stages of AI model developments. Examples include:



DATA POISONING

During the training phase: the attacker injects misleading or harmful data into the training dataset used to teach the ML model. This later degrades the model's performance and poses a major risk in terms of both security and efficiency.

ADVERSARIAL ML ATTACK

During the deployment phase: deceptive data designed to fool the classifiers is injected into the model, leading to incorrect predictions and classifications. The data is manipulated with imperceptible changes to inputs that trick the algorithm²³.



21 Artificial intelligence and cybersecurity, CEPS 2020, [URL](#).

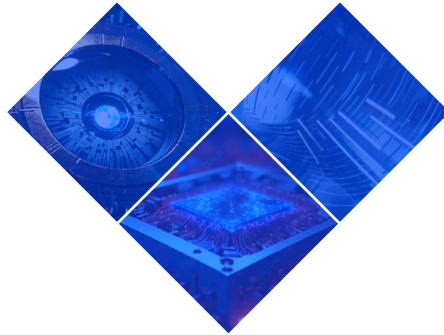
22 Artificial Intelligence and Cybersecurity Research, ENISA 2023, [URL](#).

23 Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop, National Academies 2019, [URL](#).

In addition, **AI can be used to carry out attacks against IT systems at all stages of a cyber attack**, namely the **intrusion, exploration** and **exit phases**. AI-related attacks fall into three different types: data and pattern analysis, with the enhancement of classic attacks such as malware, botnets, zero-days; **creation of synthetic data** such as false information; and **tempering**, with false results or disruption of the AI service²⁴. Some concrete examples include:

RECONNAISSANCE AND INTRUSION

AI allows attackers to gain valuable insights into the behaviour of their targets²⁵.



DATA EXFILTRATION THROUGH SECURE CHANNELS TO UNMARKED SERVERS

AI can mimic communication with social data, damage infrastructure and create botnets used for DDoS²⁷.

IDENTIFICATION OF VULNERABILITIES TO EXPLOIT, OFFERING TAILORED ATTACKS

In the exploration phase, AI can move discreetly through the network, gathering information and exploiting the compromised system²⁶.

Other ways of weaponisation of AI include **password guessing, provision of false data into the systems, hiding of activities from adversarial techniques**²⁸.

These attacks produce a **high risk of unintended consequences and errors** due to the pervasiveness of AI systems, multiple interactions and its speed of execution²⁹ which can largely increase the scope and frequency of AI-powered attacks. In an ever-more digital world where cyber threats proliferate and adversaries exploit AI maliciously, **clear guidelines for AI development in cybersecurity are imperative**. These guidelines should foster innovation while serving as a foundation to enhance cybersecurity, proactively using AI to strengthen secure IT systems.

24 Artificial Intelligence and cybersecurity: European Union panorama, da Silva Costa 2021, [URL](#).

25 Artificial Intelligence and cybersecurity: opportunities and challenges, NSTC NITRD 2020, [URL](#).

26 Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity, Taddeo 2019, [URL](#).

27 Artificial Intelligence and cybersecurity: European Union panorama, da Silva Costa 2021, [URL](#).

28 *Ibid*

29 Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity, Taddeo 2019, [URL](#).



An aerial, high-angle photograph of a busy pedestrian crossing. The crossing is marked with white diagonal stripes on a dark asphalt surface. Numerous people of various ages and ethnicities are walking across the crossing, some in groups and some alone. Their shadows are cast long and dark on the pavement, suggesting a low sun position. The overall scene is a dense, active urban environment.

The EU to the rescue – Can the EU diffuse the AI cybersecurity time bomb?

THE EU IS TACKLING AI GOVERNANCE THROUGH REGULATION BY DEVELOPING A BODY OF LEGISLATION DEDICATED TO AI SPECIFICALLY.

OVERVIEW OF EU LEGISLATION ON CYBER AND AI

The European Commission's plan "A Europe fit for the digital age³⁰" puts cybersecurity and emerging technologies such as AI at the heart of the EU's priorities. The European cybersecurity regulatory landscape has undergone major changes in recent years. AI is however barely mentioned in the texts which structure the European cybersecurity sector.

The table below summarises these efforts:

	TEXT	KEY CONTENT	MENTION OF AI
2016	Network and Information Systems Directive (NIS) <i>Regulation</i> [URL]	First EU regulation to impose a minimum level of cybersecurity in the EU to improve the Union's overall cyber-resilience by introducing cybersecurity requirements for MS, strengthening cooperation and promoting a culture of cybersecurity in critical infrastructure sectors. In particular, it distinguishes 'operators of essential services' (OESs) and 'digital services providers' (DSPs) and defines specific obligations for these entities.	No mention of AI.
2016	General Data Protection Regulation (GDPR) <i>Regulation</i> [URL]	Strengthen individuals' control and rights over personal data by providing guidelines to organisations for the collection, processing and storage of this information, with a focus on transparency, consent and mandatory reporting of data breaches.	No mention of AI.
2019	Cyber Security Act & EU Cybersecurity Certification Framework (under development) <i>Regulation</i> [URL]	Support and advance the provisions of the NIS (2016); create a legal framework for the EU Digital Single Market; remove existing barriers between MS in the digital sector and encourages cross-border commercial transactions; strengthen ENISA's mandate; and introduce a mechanism for ICT products, services and processes.	No direct mention of AI , but introduction of a certification system for products, processes and services which will have an impact on AI cybersecurity certification measures.
2020	EU Cybersecurity Strategy <i>Strategy</i> [URL]	Build resilience to cyber threats and ensure that citizens and businesses benefit from trusted digital technologies through regulatory, investment and policy initiatives in three EU policy areas: <ul style="list-style-type: none"> — resilience, technological sovereignty and leadership — operational capability for prevention, deterrence and response — cooperation to advance a global and open cyberspace. 	The first document to mention AI , it proposes the creation of a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), to form a "cybersecurity shield" to quickly detect signs of a cyberattack and take proactive measures.

30 A Europe fit for the digital age, European Commission, [URL](#).

	TEXT	KEY CONTENT	MENTION OF AI
2022	<p>Network and Information Systems Directive 2 (NIS2)</p> <p><i>Regulation</i></p> <p>[URL]</p>	<p>Clarify and extend the scope of NIS (2016) by formalising a regime of obligations and penalties for essential services providers, increasing the number of public and private organisations that must improve their level of security (with the distinction between 'essential' and 'important' entities replacing notions of OESs and DSPs), addressing supply chain security, streamlining reporting obligations and introducing stricter monitoring of implementation requirements.</p>	<p>AI is mentioned in two sections (51) and (89) of the preamble, which call for the use and integration of innovative cybersecurity technologies, including AI, to improve the prevention and detection of cyber-attacks, the management of cyber resources, and enhance the capabilities and security of critical infrastructure networks and information systems, while respecting EU data protection principles (data accuracy, data minimisation, fairness and transparency, and data security).</p>
2022 (PROPOSAL)	<p>Cyber Resilience Act</p> <p><i>Regulation</i></p> <p>[URL]</p>	<p>Provide cybersecurity requirements for products with digital components and strengthens cybersecurity rules to ensure more secure hardware and software products.</p>	<p>Art. 8 deals with high-risk AI systems and relates to the AI Act. It states that AI systems considered to have a high risk of causing harm will be deemed compliant with the cybersecurity requirements of the AI Act if they meet the essential requirements listed in the Cyber Resilience Act and demonstrate this by means of an EU Declaration of Conformity.</p>
2023 (PROPOSAL)	<p>Cyber Solidarity Act</p> <p><i>Regulation</i></p> <p>[URL]</p>	<p>Improve the preparedness, detection and response to cybersecurity incidents across the EU.</p>	<p>Promotes the development of AI and data analytics tools for improved cyber resilience and their use to provide better services and activities to the cyber community in the EU.</p> <p>Supports the creation of a European Cyber Shield, in order to improve detection capacities and timely warnings to authorities and relevant entities on EU level (19; Art. 3.2.a & Art. 3.2.e).</p> <p>Mentions the importance of pooling high-quality curated data to develop advanced AI and data analytics technologies (20).</p>

AI is only just beginning to be integrated into the wider body of European legislation and policy on cyber security, but as this table shows, it is seen more as a stand-alone issue that deserves its own body of regulations, hence the development of the AI Act.

ASSESSING THE AI ACT – DOES IT OFFER BETTER CYBER-PROTECTION?

The AI Act, which has just been adopted by the Council of the EU and the European Parliament, offers a harmonised legislative framework for the regulation of AI systems. It is the EU's first attempt at regulating all uses of AI within the Union by building excellent, secure, trustworthy and ethical AI. With this proposal, the EU is proposing a balanced approach between reaping the benefits offered by AI and preserving the Union's rights and democratic values³¹. As with the GDPR, the EU ambitions to use its normative power to provide a comprehensive AI governance framework and to set standards which could also inspire others.

The Commission proposes the adoption of a risk-based regulatory approach classifying AI systems in accordance with their level of opacity, complexity, or dependence on data. The underlying idea is to regulate the development and placement of AI systems on the EU market without imposing unnecessary restrictions which would add costs to the owners of these systems and undermine the competitiveness of the European single market³².

AI practices associated with a level of risk considered "unacceptable" will automatically be banned from the European market³³. These banned practices include predictive policing in public spaces, social scoring, real-time biometric identification or facial detection analysis. AI systems considered to present a "high risk"³⁴ will be subject to mandatory requirements before they are placed on the market, such as the registration of these systems into a EU-wide database managed by the Commission, or the conduct of self-assessment of the products³⁵.

The first mention of cybersecurity in the AI Act concerns obligations relating to high-risk AI systems³⁶. In addition to the above-mentioned practical obligations, other more general requirements apply to these systems, such as the need for transparency and the need to guarantee an appropriate level of accuracy, robustness and cybersecurity throughout the system's lifecycle. High-risk AI systems will therefore have to include solutions to prevent any exploitation of their vulnerabilities or weaponisation by malicious actors.

However, the AI Act does not focus primarily on the impact of AI on cybersecurity (or vice versa) and references to the concept of cybersecurity hardly feature in the document. Although some of its provisions may indirectly contribute to improving cybersecurity, AI and cybersecurity continue to be treated as separate issues in EU regulation. That said, the AI Act could contribute to improving cybersecurity in the following ways:

31 Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021, [URL](#).

32 *Ibid* (context of the proposal)

33 *Ibid* (Title II article 5)

34 *Ibid* (Title III, chapter 1, article 6)

35 *Ibid* (Title III, Chapter 2)

36 *Ibid* (Title III, Chapter 2, article 15)

- Stricter requirements for high-risk AI systems, including ensuring a risk-appropriate level of robustness, accuracy and cybersecurity
- Emphasising data governance and security, which are necessary for effective cybersecurity
- Promoting transparency and accountability, providing users with information about the capabilities and limitations of AI systems, and thus influencing decision-making in relation to cyber risks.

While the AI Act is the first of its kind, and has been widely welcomed on the international stage, many have already raised concerns and proposed amendments, calling for substantial changes, particularly in terms of consumer protection, or more simply to criticise the impact of on innovation, particularly for SMEs. The AI Act could be costly for the EU in terms of money, but also in terms of innovation and competitiveness. Studies estimate that the EU could lose €31 billion over the next five years and that investment in AI could be cut by almost 20%³⁷.

One question will be whether the AI Act could have a positive impact on cybersecurity solution providers in particular. Like the GDPR, which helped develop a market for cybersecurity privacy, the AI Act could also spur innovation, forcing companies to create new tools and perhaps even encouraging R&D. Bringing companies up to date with the EU regulation could therefore represent a significant cost for those who must comply, but also offer significant market opportunities.

37 Study warns of compliance costs for regulating Artificial Intelligence, Euractiv 2021, [URL](#).



A photograph of a gallery space. A large, solid black circle is mounted on a dark green wall. The wall is flanked by white walls, and the floor is a dark, reflective surface. The ceiling features exposed pipes and structural elements. The overall lighting is dramatic, highlighting the central circle.

**WAY
FORWARD**

Understanding the intricacies of a technology is not a prerequisite for its use, and this principle applies to AI in the field of cybersecurity. It would be foolish to forego a substantial opportunity to take advantage of such a powerful technology or, conversely, to subject it to excessive regulation, thereby falling behind on the world stage where rival powers do not all play by the same rules.

Europe must remain at the forefront of AI innovation for cybersecurity, adopting a pragmatic perspective which harnesses the benefits of AI to keep pace, encourage innovation and, above all, assert its own influence in the evolution of AI. Ultimately, the crucial issue is not just the mechanisms and functionalities of the technology, but rather the strategic use we make of it and the choices we make about its application.



The key issue here is distinguishing the technology from its use. AI is inherently neither good nor bad, its uses should instead be the focus. In the end, AI is simply a technology which requires the development of an appropriate and secure processes and systems to yield benefits.

As a result, the following recommendations provide some food for thought as to how to improve AI for cybersecurity in the EU:



UNDERSTAND THE THREAT LANDSCAPE

Frequent analysis of the lifecycle of AI systems, including their operational requirements and potential threats and vulnerabilities, is the basis for effective governance (adaptation to constantly changing environments, enhanced security, operational efficiency, etc.).



ESTABLISH CLEAR STANDARDS AND GUIDELINES TO GOVERN THE USE OF AI IN CYBERSECURITY

Clear standards and guidelines for the use of AI in cybersecurity (and beyond) provide a structured framework that ensures the responsible use of AI. Regulators thus address potential risks and concerns while providing clarity, allowing stakeholders to innovate within well-defined boundaries.



CONDUCT PERIODIC ASSESSMENTS

Periodic evaluations of the effectiveness of the measures introduced by the AI Act would ensure that they remain up to date and fit for purpose in light of evolutions of both the technology and its uses.



SUPPORT INDUSTRY ADAPTATION

Support European companies as they adapt to AI-based solutions, including compliance by solution providers and users.



BOOST RESEARCH AND DEVELOPMENT FOR THE AI-CYBERSECURITY NEXUS

Encourage R&D through EU-funded programmes aimed at all sectors impacted by AI and cybersecurity (DEP, EDF, Horizon Europe, etc.).



PROMOTE PUBLIC AWARENESS AND EDUCATION

Citizens are the weakest link in cyber security - and they could become the weakest link in AI. Raising awareness and educating them about technology is essential to understanding the risks and benefits, promoting effective use and strengthening cyber resilience as a whole.

BIBLIOGRAPHY

- A Europe fit for the digital age, European Commission, [URL](#).
- AI in cyber security: benefits and uses cases, Altamira 2023, [URL](#).
- Artificial Intelligence Act, European Parliament, [URL](#).
- Artificial Intelligence and Cybersecurity Research, ENISA 2023, [URL](#).
- Artificial intelligence and cybersecurity, CEPS 2020, [URL](#).
- Artificial Intelligence and cybersecurity: European Union panorama, da Silva Costa 2021, [URL](#).
- Artificial Intelligence and cybersecurity: opportunities and challenges, NSTC NITRD 2020, [URL](#).
- Artificial intelligence for cybersecurity: Literature review and future research directions, Kaur et al. 2023, [URL](#).
- Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution, oosen et al. 2018, [URL](#).
- Attacking artificial intelligence: AI's Security Vulnerability and What Policymakers Can Do About It, Comiter 2019, [URL](#).
- Cloud computing - statistics on the use by enterprises, Eurostat 2023, [URL](#).
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, [URL](#).
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), [URL](#).
- Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop, National Academies 2019, [URL](#).
- Incident response automation: What it is and how it works, Irei and Froehlich 2023, [URL](#).
- Joint communication to the European Parliament and the Council, The EU's Cybersecurity strategy for the Digital Decade, 2020, [URL](#).
- Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021, [URL](#).
- Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, [URL](#).
- Proposal for a regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, [URL](#).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [URL](#).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), [URL](#).

Study warns of compliance costs for regulating Artificial Intelligence, Euractiv 2021, [URL](#).

The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, Ansari et al. 2023, [URL](#).

Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity, Taddeo 2019, [URL](#).

Timeline - Artificial intelligence, Council of the EU, [URL](#).

Une année 2021 marquée par la professionnalisation des acteurs malveillants, ANSSI 2022, [URL](#).

X-Force threat intelligence index, IBM 2023, [URL](#).



RETROUVEZ NOS DERNIÈRES ACTUALITÉS
ET NOS PROCHAINS ÉVÉNEMENTS SUR :

agora-fic.com