Regulatory Challenges in Cybersecurity – A Critical Analysis of the EU AI Act

Fédéric Tronnier[1][0000−0002−6202−4871], Sascha Löbner[1][0000−0001−9164−1919], Marie-Hermance Lacombe[1][0009−0007−8858−933X], and Kai Rannenberg[1][0009−0000−6142−7161]

Goethe University Frankfurt am Main, Germany frederic.tronnier@m-chair.de

Abstract. The recently enacted European regulation on Artificial Intelligence (AI), the AI Act, seeks to mitigate risks associated with AI systems and to protect fundamental rights while promoting innovation within the European Union (EU). For cybersecurity educators and professionals, Article 4 of the AI Act promotes the tremendous challenge of obliging organizations that use AI systems to educate their employees on the subject, in order to promote AI literacy. This article therefore provides a systematic literature review on the AI Act and its criticisms, with the intention of fostering an understanding of the challenges ahead, by providing an educational overview on the subject of AI regulation. We find research on the AI Act from a cybersecurity perspective to be scarce. The results of our review demonstrate that the Act has faced significant criticism for its lack of clarity and the challenges of concrete application, stemming from the complexity of algorithms and the diverse range of sectors it encompasses. The complexity of implementation of the regulation hinders compliance and, overall, innovation, leaving several opportunities for regulatory improvement and academic research.

Keywords: AI Act · Security · Cybersecurity Regulation · Artificial Intelligence Regulation

1 Introduction

Artificial Intelligence (AI) is seen as the driver of the next worldwide revolution, affecting researchers, information and computer science professionals as well as experts on cybersecurity and cybersecurity education. AI, Large Language Models (LLMs) and machine learning (ML) are seemingly mixed, offering possibilities hitherto unimagined, yet it is up to regulators to provide order and structure where previously chaos ruled. In less than a decade, AI has undergone rapid advancements and has emerged as a critical force shaping our societies at an accelerating pace. Consequently, this acceleration culminated in a surge of public and private interest. Indeed, as AI continues to disrupt industries, governments recognize its potential to revolutionize areas like healthcare, education, or finance, while also acknowledging risks to privacy and cybersecurity. The reliance of ML systems on vast data sets presents a variety of ethical and legal challenges,

e.g. through a lack of accountability, fairness and transparency, highlighting the need for clear guidelines.

Aware of the scale of these concerns and with the ambition of ensuring excellence in the field, the European Union (EU) has adopted a strategic approach, aiming to position itself as a pioneer in the regulation of AI. This ambition involves establishing standardized norms and rules to govern the behavior of the many actors, in order to safeguard individual privacy and security and ensure that AI systems align with societal values. The European Commission (EC) implemented legislative initiatives such as the General Data Protection Regulation (GDPR) in 2018, which aims to protect the confidentiality of personal data and guarantee the privacy of EU citizens. It introduced transparency and information requirements, which were later complemented and formalized in the specific field of AI by the AI Act, which came into force in August 2024. The Act seeks to mitigate risks associated with AI technologies and to ensure its secure and ethical use across various sectors. It aims to regulate AI as a whole, ensuring trust, in order to foster innovation among the EU while protecting fundamental rights. However, the implementation of these regulations is complicated by the complexity of ongoing technical innovation and the diversity of applicable sectors. Considering the recency of the regulation, the objective of this work is therefore to provide a comprehensive overview of the existing literature on the scope and the limitation of EU AI Act. A specific focus is put on the field of cybersecurity. The results aim to provide guidance and orientation for the continuous improvement of AI regulation, and depict the status quo of research on the AI Act for cybersecurity professionals that will be affected by the implementation of the Act. Thus, this work addresses the following research question:

RQ: *What limitations, challenges and gaps have been observed in the AI Act?*

In the following, the second section provides background information on the AI Act and its link to cybersecurity education. Section three introduces the methodology, a systematic literature review following [3]. The results are then presented in section 4. This work concludes with a summary of the identified challenges, while outlining limitations as well as areas for future research.

2 The AI Act and its Link to Cybersecurity Education

The European Commission's definition of AI in the AI Act (Art. 3 AI Act) emphasizes the autonomy of systems. Concretely, the AI Act mainly targets AI applications that rely heavily on algorithms using ML. As ML systems become increasingly integrated into various aspects of society, their socio-technical implications are becoming more apparent. The use of ML systems has raised significant concerns [33], e.g. surrounding data usage [11]. Consequently, the widespread adoption of AI and ML across sectors can lead to harmful consequences if ethical concerns are not addressed [34]. To address such concerns, the EU AI Act, proposed in 2021 and in force since August 2024, establishes a risk-based regulatory framework to mitigate potential harm arising from the use of

AI systems. Unlike the GDPR, which applies to all automated decisions affecting individuals, the AI Act focuses exclusively on AI systems, categorizing them based on their potential detrimental impacts on health, safety, and fundamental rights. These legal regimes cover four clusters of AI systems with (i) unacceptable (severe), (ii) high, (iii) limited, and (iv) minimal risks. This classification ensures tailored regulatory approaches to manage the risks associated with different AI uses effectively. The AI Act integrates ethical considerations aimed at promoting AI development while safeguarding human rights and values. It contains a closed list of prohibited AI practices associated with AI systems which are rated with Unacceptable-Risk (Art. 5 AI Act). These are AI systems that pose clear threats to human safety, dignity or rights. Limited-risk AI systems need to comply with transparency obligations defined in the regulation. AI systems whose risk is deemed minimal can follow a voluntary code of conduct defined in the Act. The AI Act primarily focuses on high-risk systems, which pose a greater potential threat to society, categorizing them in two types (Art. 6 AI Act): (i) AI intended to be used as a product covered by specific EU legislation, such as civil aviation, and (ii) AI systems listed in Annex III of the AI Act, such as systems for law enforcement and education and vocational training. Providers of high-risk AI systems must meet strict requirements to ensure that their AI systems are trustworthy, transparent and accountable (Chap. III AI Act). Particularly important for cybersecurity professionals are the obligations introduced in the Act. They must conduct risk assessments (Art. 9 AI Act), use high-quality data (Art. 10 AI Act), document their technical and ethical choices (Art. 11), keep records of their system's performance (Art. 12 AI Act), inform users about the nature and purpose of their systems (Art. 13 AI Act), enable human oversight and intervention, and ensure accuracy, robustness, and cybersecurity (Art. 14 AI Act). They must also test their systems for conformity with the rules before placing them on the market or putting them into service, but they also have to establish a post-market monitoring system (Art. 72 AI Act). As transparency in AI systems is a major point of the act, accountabilities are shifted at all stages along the value chain imposing strict obligations not only on the 'provider' of a high-risk AI system, but also on the 'importer', 'distributor' and 'deployer' of such systems (Chap. III-Section 3 and Chap. 4 Art. 50 AI Act).

Several comments and opinions were published throughout the development process of the AI Act. De Cooman [7] argues the AI Act's deficiency in addressing the full range of risks associated with AI systems by referring to the potential harms of non-high-risk AI, i.e. AI systems with limited or minimal risk. The author also highlights the importance of culture and social tolerance in determining harmful applications of AI. Gyevnar et al. [15] argue that there is a lack of concrete mechanisms to ensure real explainability of AI systems. The transparency requirements defined by the Act are likely to remain superficial without clear criteria for explainability and robust audit measures. Scantamburlo et al. [31] evaluated the challenges of determination of risk level in AI systems. Their report includes a critical evaluation of legal requirements, and urgent recommendations to help providers achieve compliance.

In the context of cybersecurity education, the AI Act needs to be addressed from two main perspectives. Firstly, AI systems and solutions are increasingly being used for cybersecurity purposes, as well as for cybersecurity education. For instance, the authors of [1] use Generative Pre-Trained Transformers (GPT) to create tailored and dynamic cybersecurity training material. The results indicate the solution's applicability in enhancing cybersecurity awareness. As another area of application, [20] study the applicability of AI chatbots for career counselling for cybersecurity professionals. Such work thereby corresponds to Recital 56 of the AI Act which aims to foster the use of AI for educational purposes by stating that *"the deployment of AI systems in education is important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes. [...] When improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination [...] " (Recital 56 AI Act)*. As observed, the Recital highlights the need for caution when introducing AI for educational purposes, which further emphasizes the need for more research on both, AI systems and the AI Act in ensuring security. This serves as a motivation for this work. Secondly, cybersecurity researchers and practitioners need to work on mitigating threats and risks of AI applications, while being aware of the requirements set forth by the corresponding regulation: *"Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used." (Art.4 AI Act)*. Thus, cybersecurity education is seen as an incremental task when working with AI systems. Therefore, we investigate the AI Act in more detail, aiming to find whether and how cybersecurity research is currently addressing the AI Act.

3 Methodology

Our research fills the identified gap in academic research by conduction a systematic literature review on the scope, limitations and issues with respect to the implementation of the AI Act, following its introduction. The aim of this work is to provide a comprehensive overview of on the topic at hand. Thus, the recency of our articles found was set as a priority. To conduct a systematic literature review, we followed the guidelines and best practices provided by Brocke et al. [3]. In accordance with the taxonomy of Cooper [6], the goal is to structure existing criticism towards the AI Act as well as to define central issues with and of the regulation. In doing so, we focus on research outcomes rather than research theories. The coverage is to be seen as representative, while the perspective is espousal of position. The target audience are general scholars

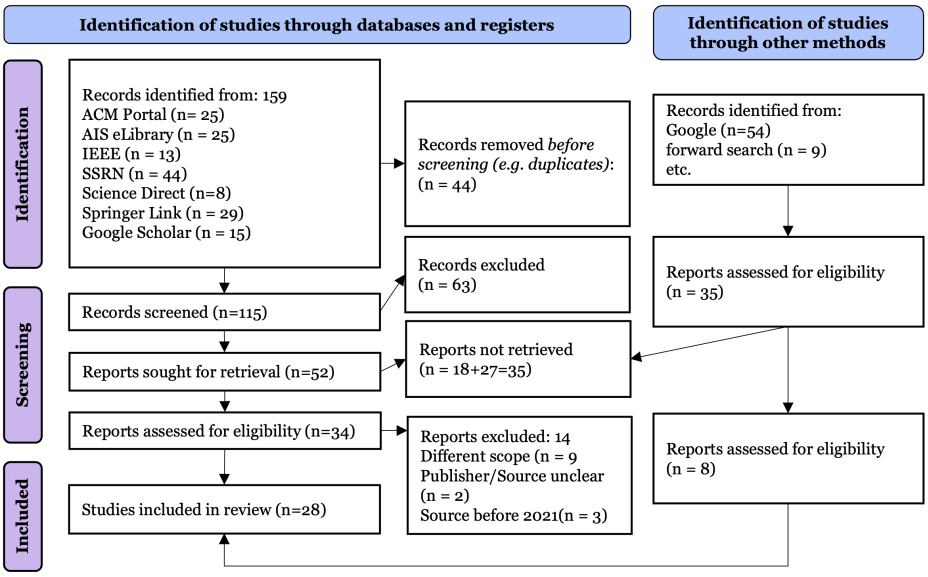

Fig. 1. PRISMA literature review process, following Page et al. [26]

and practitioners, interested in the application and limitations of the AI Act, in the context of cybersecurity. We utilized the PRISMA 2020 checklist [26] as a framework to report our literature identification process. The focus on the AI Act and its relation to cybersecurity education guided the research process. However, too few articles met these initial criteria. Therefore, the scope was broadened towards cybersecurity and the AI Act in general, by also including few additional information sources from academic and legal blogs and websites. The database used to analyse the official regulatory texts from the European Commission was EUR-Lex, as well as the official sites of the DGPR and the AI Act. The scientific databases consulted to identify relevant academic studies were ACM Portal, Google Scholar, IEEE Xplore Digital Library, Science Direct, AiS Library, Science Direct, Springer Link and the SSRN platform. The term "AI Act" was included in all search queries. Key additional search inputs included the following keywords: "AI Act analysis", "AI Act regulation" and "AI Act AND cybersecurity". 28 final hits emerged that were selected for our analysis in the results section. The most relevant studies were chosen based on a critical analysis of the AI Act applied to general cases, ensuring a representative sample of the respective domains. The detailed PRISMA flowchart illustrating the selection process is provided in Figure 1. We used the concept-centric approach by Webster and Watson [37] to analyse trends and key concepts highlighted in each of the selected articles.

4 Results

Table 1 provides an overview of the occurrence of different observations and identified limitations of the AI Act across the relevant literature. The results depict the identified domain of research in which the obtained articles were conducted. Individual articles were often located at the interface between two or more research domains, for example in cybersecurity law journals, which represent the intersection between legal and information technology research. In addition, the presumed addressee of the article is indicated by the perspective of the article. It can be seen that many articles are aimed at regulators or policymakers, while only a few articles are addressed to academics or companies, or consider their perspective on the AI Act. The common thread running through all articles is a dedicated analysis of the AI Act and its regulatory challenges. Trends and notions mentioned in the reviews were recurrently noted, enabling them to be classified into generalized categories. If a paper focuses or discusses one of the aggregated categories, we indicate it with an "✔" in Table 1. In the following, the main identified research themes are discussed.

4.1 Ambiguity of definitions and scope

The first category of findings in Table 1 refers to the lack of clarity in the definition of terms and requirements outlined by the AI Act and was the topic identified most frequently in the reviewed literature. The current regulation is criticized by multiple identified articles for creating ambiguity and uncertainty due to overly broad definitions of legal status that necessitate clarification. Gyevnar et al. [15] refer to the mismatch of views as "the transparency gap" which argues that the definitions, scope and purpose of transparency in regulations are not in agreement with how technological approaches understand them. Policymakers view transparency as a mean that supports wider values such as accountability, human rights, and sustainable innovation. In contrast, explainable AI (XAI) views transparency narrowly as an end in itself, focusing on explaining complex algorithmic properties without considering the socio-technical context. This difference leads to challenges in aligning technical applications with regulatory requirements. Musch et al. [24] underline the lack of direct translation of the instructions described in the regulations into concrete process. Consequently, this unclarity can leave room for interpretation, weakening its implementation across stakeholders of the value chain of systems but also across member states [8]. Moreover, according to the scenarios, the question of legal responsibility between developers, providers, and users is not fully resolved by the AI Act. Yet, they are necessary to prevent damage caused by AI systems if too many liberties are taken, to avoid undermining stakeholder trust, and prevent negative impacts on innovation [38]. Clarifying accountability is crucial, particularly when it comes to opaque ML algorithms like black boxes, where the risk of error is inherent. The question of responsibility for the results arises further when it comes to unintelligible probabilistic models [22]. Ruschemeier [30] provides an exemplary work on the challenge of regulating AI. The authors discuss how AI

Table 1. Classification of literature by research domain, perspective and identified issues with the AI Act.

Literature	*Lack of clarity*	*Risk assessment challenges*	*Conflicts/ gaps in standards*	*Competitive disadvantages*	*Technical challenges*	*Organizational challenges*	*Self-governance challenges*	*Research domain*	*Perspective*
[2]						✓		Legal	Policymaker
[4]	✓		✓		✓	✓		Non-scientific	Policymaker
[5]			✓					Legal	Policymaker
[8]	✓			✓		✓	✓	Business	Organizational
[9]	✓				✓	✓		Non-scientific	Policymaker
[10]	✓	✓		✓	✓		✓	Legal	Policymaker
[12]	✓			✓		✓		Non-scientific	Policymaker
[13]						✓	✓	Information Systems	Organizational
[14]	✓		✓					Informatics	Societal / Research
[15]	✓	✓			✓		✓	Informatics	Academic Research
[16]		✓		✓	✓			Non-scientific	Policymaker
[17]	✓	✓	✓			✓		Information Systems	Organizational
[19]						✓		Information Systems	Organizational
[18]		✓	✓			✓		Legal	Organizational
[21]		✓			✓		✓	Politics	Societal
[22]	✓	✓			✓	✓		Information Systems	Organizational
[23]	✓							Legal	Policymaker
[24]	✓	✓			✓	✓		Ethics	Societal
[25]	✓	✓				✓	✓	Legal	Policymaker
[27]	✓		✓			✓		Legal	Policymaker
[28]					✓		✓	Informatics	Policymaker
[29]		✓	✓		✓	✓		Non-scientific	Organizational
[30]	✓							Legal	Policymaker
[31]	✓		✓		✓	✓		Informatics	Organizational
[32]	✓	✓		✓				Legal	Policymaker
[35]	✓	✓			✓		✓	Legal	Policymaker
[36]	✓	✓	✓	✓		✓	✓	Legal	Organizational
[38]	✓	✓	✓	✓				Non-scientific	Societal
$\sum$	19	14	10	7	12	16	9		

can be regulated, given the constantly evolving topic and a plethora of differing definitions of AI. A solution mentioned by White [38], although purely theoretical, is then to start attributing legal personality to AI. Therefore, the author

is optimistic about the AI Liability Directive (AILD), a proposal introduced by the European Commission in 2022 that aims to clarify the legal responsibilities of parties involved in AI systems.

4.2 Risks and risk classification

The second category of identified findings criticizes the risk classification of the AI Act, which is deemed to be too static, causing the omission of certain AI systems, particularly those deemed "low-risk", yet still capable of generating significant social, ethical, or psychological consequences [36]. Therefore, the AI Act does not capture the full scope of consequences, neglecting intangible impacts such as systemic discrimination particularly linked with algorithmic bias of ML models. According to the author, one danger of the Act is that it creates "grey areas" in the regulation, leaving many harmful applications outside the regulatory scope. As Ebers et al. [10] point out: "The Commission should avoid what this article humorously labels as the Humpty Dumpty fallacy. Just because the Proposal dichotomizes high-risk and non-high-risk AI systems does not mean the latter are not worthy of discussion." Even the categorization of "high-risk" AI systems is considered "unduly blunt and simplistic" [32]. Indeed, high-risk AI systems may still be deployed even if they interfere with fundamental rights, if those deploying them adhere to the requirements set out under Chapter III. The protection afforded by the Act hence entirely depends on whether the closed 'high-risk list' provided in Annex III, is sufficiently comprehensive and up to date. But, according to the authors, this demand may be hard to meet, especially given the technology's evolving nature. In addition to the complexity of preemptively assessing the risks, another major challenge lies in concretely applying the risk-based approach. The Act does not cover all algorithmic methods encompassed by ML. As a matter of fact, it overlooks a crucial technological aspect, particularly in Article 10, by limiting the scope of requirements to training, validation, and testing data. While datasets are undeniably critical for data-driven AI systems, such as reinforcement learning, methods like planning and reinforcement learning do not rely on the same techniques as supervised learning, from which these terms originate. It remains unclear what requirements should be met for systems that rely on the input data of such methods to generate their explanations. [15]. For more complex types of ML algorithms, compliance with these requirements becomes even more challenging, particularly in monitoring system quality and managing bias and discrimination due to their complexity and opacity. Scantamburlo et al. [31] point out that applied to even more general- purpose AI systems, the compliance process becomes rather complicated due to their potential for diverse purposes. Delegating the responsibility of defining permissible uses to providers, along with the corresponding obligations for compliance of potentially harmful systems, raises legitimate concerns. Therefore, the establishment of more precise criteria is deemed necessary to define which requirements a system is subject to and what constitutes the validity of the different requirements. To address the multiple and changing high-risk classifications and the unknown land of AI risks, Golpayegani et al. [14] developed an open resource vocabulary

for AI risks (VAIR) to represent and assist with AI risk assessments of systems that respect Annex III conditions and help with documentation. VAIR is intended to facilitate the Ai acts applicability by providing a common vocabulary that facilitates knowledge sharing and connectivity between stakeholders in the AI value chain. A set of guiding principles for cybersecurity requirements for high-risk AI systems is provided by [18] of the Joint Research Centre (JCR) as a service by the European Commission. It aims to address some of the challenges and limitations in this work by providing a high-level assessment of the AI Act.

4.3 Missing coordination of standards and regulation

To ensure the AI Act's effectiveness in achieving harmonization, legal challenges arise from the coordination with existing standards. This issue falls under the third category of 1. Indeed, current standards, such as industry-specific standards, need to be adapted. Heidemann et al. [17] illustrate this point using existing road-vehicle safety standards that align well with Article 9 of the EU AI Act but provide weaker coverage than the act of certain requirements for human oversight and transparency. Quintais [27] provide a legal analysis with respect to copyright issues when dealing with Generative AI and the interaction between the AI Act and EU copyright law such as the Digital Single Market Directive (CDSMD). Similarly, the first challenge highlighted by Scantamburlo et al. [31] in their analysis of the AI Act, is the conflicts arising from potential coordination issues with existing legal frameworks, such as competition law and consumer law. Assessment requirements can lead to challenges involving more extensive considerations, such as intersections with other legal obligations (e.g., GDPR, Copyright Law). The transparency mandated by the GDPR and further reinforced by the AI Act also necessitates the disclosure of specific system techniques. The article of Fernhout and Duquin [12] takes the example machine learning algorithms used for credit scoring, classified as high-risk system. The economic model and competitive advantage of these systems rely on the precise weightings and parameters, which are protected as trade secrets. Under the transparency requirement, there is a risk of infringing proprietary rights by requiring the disclosure of motivations and design decisions. This could reveal detailed information about the algorithms and data used, thereby affecting intellectual property, trade secrets, and competitive advantage. Casarosa [5] follows this conclusion by stating that the missing alignment between the AI Act and another regulation, the Cybersecurity Act, is to be seen as a missed opportunity, as "different approaches adopted in the two acts may undermine the goal of certification mechanisms as trust-enhancing and transparency instruments". In the cybersecurity domain, the missing coordination between different regulations is also discussed through the discussion of the Network and Information Security System Directive reform (NIS 2), whereby Biasin and Kamenjašević [2] reach the same conclusion as [5]. At the time of writing, no specific standard was introduced for the certification of AI systems. And some of the already available standards, technical specifications, and technical reports proposed by the ISO are insufficient and are often criticized for failing to meet the requirements of the

AI Act. For example, there is a divergence in approach between the requirements of the AI Act and the ISO/IEC 23894 standard, titled "Artificial Intelligence — Guidance on Risk Management," which aims to guide organizations in managing AI system risks. This standard primarily focuses on internal risks to the organization developing AI. However, the AI Act, as outlined in Article 9, takes a broader view of risk management, considering external risks such as health, safety, and the fundamental rights of individuals affected by AI systems. In [14], the authors map the standardization activities undertaken by the committee ISO/IEC JTC 1/SC 42 to the high-risk AI requirements. The conclusions highlight that: (i) there is a lack of standards for technical documentation (Art. 11 AI Act), user instructions (Art. 13 AI Act), and record-keeping management (Art. 12 AI Act); (ii) there is a shortage of certifiable organizational standards. Most standards are primarily designed to provide guidelines b, but not yet offer precise and measurable criteria for official certification. Without certifiable standards, proving that AI systems comply with legal requirements will be challenging, even if those standards are followed; (iii) access to current ISO standards is costly, which creates a barrier that disadvantages smaller organizations (startups, SMEs, research institutions). Requests for standardization are expected to be issued by the European Commission (Art. 40 AI Act). Other organizations like the AI Watch have started to propose a preliminary roadmap of international standards in support of the requirements set out by the AI Act. [31] propose the adaptation of existing standards, such as ISO/IEC TR 24368:2022 for describing technical specifications for the assessment of machine learning classification performance.

4.4 Challenges relating to the implementation of the AI Act

The compliance process is hindered by the complexity of the organizational implementation of the AI Act requirements. By trying to comply, AI providers could face shortages in human resources, technical expertise, as well as financial resources, especially when adhering to paid standards. For instance, it is foreseen that deployers of high-risk AI systems must implement human oversight, monitoring, and report serious incidents and malfunctions, adding to operational costs [8]. These requisites may carry a premium, potentially leading to higher prices for consumers. Moreover, meeting EU AI Act requirements may increase administrative burdens, delaying and discouraging the launch of new AI products or updated versions. Gengler and Schmalenbach [13], Kahdan et al. [19] assess the AI Act from an organisational point-of-view. By observing the response behaviour of 400 organizations, [19] derive four distinct response strategies, circumvent, comply, compromise, and control, as well as multiple response practices towards AI regulation. Similarly, Ramos and Ellul [28] provides one of the few works on the AI Act from a cybersecurity perspective. The authors argue that the utilization of blockchain technology may aid in complying with some of the AI Act requirements on data governance, transparency and record keeping. Furthermore, several authors argue that time-consuming and costly processes could favour large companies at the expense of smaller ones, because of their greater resources and advanced expertise, creating a competitive disadvantage [25]. But,

the EU AI Act could also discourage the development of AI solutions by affecting international competition with regions that are not subject to such regulations [8]. An interdisciplinary collaboration mechanism between the public and private sectors has been proposed to promote a holistic approach to allow a better application of the overly rigid framework to different AI use cases [31]. However, this collaboration is often seen as lobbying, facilitating the self-governance process of large technology companies. Accused of "secret negotiations" by Metikos [23], it is claimed that policymakers allowed and favour the influence of Big Tech lobbyists during the legislative process of the AI Act. It cites the French company Mistral, which opposed the regulation of generative AI to defend its own interests. This illustrates the need for balanced cooperation between legislators and the private sector, to avoid excessive lobbying and compelling self-governance.

5 Discussion

The main challenges and issues raised by researchers with the AI Act may be grouped into three categories: (i) First, the lack of clarity in the definitions of used terms, the lack of precision in the risk-classification of AI systems, the unclear definition of the necessary requirements, and the lack of clear legal responsibilities assigned to the various stakeholders. (ii) The gap and partly overlap between existing regulations and the absence of certifiable standards. (iii) The technical and organizational difficulties in applying the regulation, which may slow down its implementation and act as a competitive disadvantage for organisations. By providing an overview of ongoing trends in critiques of the AI Act, these results confirm the concerns raised regarding existing regulations. For instance, the financial and organizational resources required could risk stifling innovation by favouring large, influential companies capable of mobilizing such resources to shape the legal framework to serve their own interests. As a result, this could distort competition and discourage overall AI innovation. Thus, this analysis highlights the need to adapt future regulations to ensure their applicability to the entire market and alignment with the complexity of AI systems. A first step in addressing particularly the identified lack of clarity (i), could be the Code of Practice, for which the EC will start its drafting process in Mai 2025.

Naturally, this work is not without limitations. The literature review process did only identify a representative set of findings, more work might be found in other domains, e.g. in legal or ethics databases. The potential presence of reporting bias need to be acknowledged, as does the lack of further analysis of the identified authors and their geographic and institutional perspectives that may explain their criticism. Nonetheless, for cybersecurity researchers, the lack of findings specifically tailored towards cybersecurity education, demonstrate the need for future research in this domain. Not only does AI regulation need to keep track with the rapid evolution of AI, but researchers need to keep track as well. Cybersecurity educators need to be aware of the regulation to identify strategies to educate AI system deployers as well as AI system users on the subject. As of now, research is found to focus strongly on a legal interpretation of the Act, by

providing research from the perspective of a policymaker. Future work should therefore assess how exactly cybersecurity educators can comply with the AI Acts requirements on AI literacy, for instance by developing quality standards for AI education in different organisational and societal domains.

6 Conclusion

This work provides a systematic literature review on the recent AI Act, which aids cybersecurity professionals in understanding the current challenges and limitations of a regulation that might severely impact their daily work. In the context of cybersecurity, this work highlights current shortcomings with respect to the scope and applicability of the regulation, as well as challenges in the identification and classification of risks. According to the discussed research, the AI Act does not to adequately address the challenges posed by AI and ML systems. For cybersecurity educators, the AI Act will be another regulation to be considered, as the AI Act clearly emphasizes the importance of educating personnel on AI applications, systems and it's functioning. Therefore, future work should study not only study how cybersecurity education can be facilitated through AI [1, 20], but how cybersecurity education on AI itself can be fostered, and AI compliance be achieved in a multi-perspective environment.

Acknowledgments. This article was co-funded through the FIIPS-at-Home project, funded by the German Federal Ministry of Education and Research under (funding code 16KISA068K) and CyberSecPro (Project Agreement no. 101083594), co-funded by the European Union. Responsibility for the contents lies with the authors.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Al-Dhamari, N., Clarke, N.: GPT-Enabled Cybersecurity Training: A Tailored Approach for Effective Awareness. In: IFIP World Conference on Information Security Education, pp. 3–20, Springer (2024)
2. Biasin, E., Kamenjašević, E.: Cybersecurity of medical devices: new challenges arising from the ai act and nis 2 directive proposals. International Cybersecurity Law Review **3**(1), 163–180 (2022)
3. Brocke, J.v., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., Cleven, A.: Reconstructing the giant: On the importance of rigour in documenting the literature search process (2009)
4. Caroli, L.: Will the EU AI Act work? Lessons learned from past legislative initiatives, future challenges. International Association of Privacy Professionals (2024)
5. Casarosa, F.: Cybersecurity certification of artificial intelligence: a missed opportunity to coordinate between the artificial intelligence act and the cybersecurity act. International Cybersecurity Law Review **3**(1) (2022)

6. Cooper, H.M.: Organizing knowledge syntheses: A taxonomy of literature reviews. Knowledge in society **1**(1), 104 (1988)
7. De Cooman, J.: Humpty dumpty and high-risk AI systems: the ratione materiae dimension of the proposal for an EU artificial intelligence act. Mkt. & Competition L. Rev. **6**, 49 (2022)
8. Ditsche, J., Mikhaylenko, M.: European AI Act: Opportunities and challenges (May 2024), retrieved from rolandberger.com
9. Djeffal, C.: The EU AI Act at a crossroads: generative AI as a challenge for regulation. European Law Blog (2023)
10. Ebers, M., Hoch, V.R., Rosenkranz, F., Ruschemeier, H., Steinrötter, B.: The European Commission's proposal for an Artificial Intelligence Act—a critical assessment by members of the Robotics and AI Law Society (RAILS). J **4**(4), 589–603 (2021)
11. El Mestari, S.Z., Lenzini, G., Demirci, H.: Preserving data privacy in machine learning systems. Computers & Security **137**, 103605 (2024)
12. Fernhout, F., Duquin, T.: The EU Artificial Intelligence Act: Our 16 Key Takeaways (February 2024), retrieved from stibbe.com
13. Gengler, E., Schmalenbach, K.: Exploring organizational ai governance maturity: A case study with six multinational companies. In: Proceedings of the International Conference on Information Systems (ICIS), AiS (2024)
14. Golpayegani, D., Pandit, H.J., Lewis, D.: To Be High-Risk, or Not To Be—Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards. In: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency (2023)
15. Gyevnar, B., Ferguson, N., Schafer, B.: Bridging the Transparency Gap: What Can Explainable AI Learn From the AI Act? In: ECAI 2023, pp. 964–971, IOS Press (2023)
16. Hacker, P.: What's Missing from the EU AI Act. Verfassungsblog: On Matters Constitutional (2023)
17. Heidemann, L., Herd, B., Kelly, J., Mata, N., Tsai, W.T., Zafar, S.A., Zamanian, A.: The European Artificial Intelligence Act (2024)
18. Junklewitz, H., Hamon, R., André, A., Evas, T., Soler Garrido, J., Sanchez Martin, J.: Cybersecurity of artificial intelligence in the ai act. Publications Office Eur. Union (2023)
19. Kahdan, M., Hartwich, N.J., Salge, O., Cichy, P.: Navigating Uncertain Waters: How Organizations Respond to Institutional Pressure in Times of the Looming EU AI Act. In: Proceedings of the International Conference on Information Systems (ICIS), AiS (2023)
20. Koukou, C., Stavrou, E.: The Potential of Generative AI Chatbots as Career Advisors in Cybersecurity: Professionals' Perspectives. In: IFIP World Conference on Information Security Education, pp. 191–206, Springer (2024)
21. MacCarthy, M., Propp, K.: Machines learn that Brussels writes the rules: The EU's new AI regulation. Brookings, May **4**, 2021 (2021)
22. Maxwell, W., Caulier, S.: "AI Act", comment l'Europe veut réguler les machines. Polytechnique Insights (Dec 2021)

23. Metikos, L.: The AI Act: Weak, Weaker, Weakest. Ljubiša Metikoš, Mediaforum **3**, 73–74 (2024)
24. Musch, S., Borrelli, M., Kerrigan, C.: The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development. SSRN 4549248 (2023)
25. Outeda, C.C.: The EU's AI act: a framework for collaborative governance. Internet of Things p. 101291 (2024)
26. Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., et al.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. bmj **372** (2021)
27. Quintais, J.P.: Generative ai, copyright and the ai act. Computer Law & Security Review **56**, 106107 (2025)
28. Ramos, S., Ellul, J.: Blockchain for artificial intelligence (ai): enhancing compliance with the eu ai act through distributed ledger technology. a cybersecurity perspective. International Cybersecurity Law Review **5**(1), 1–20 (2024)
29. Renieris, E.M., Kiron, D., Mills, S.: Organizations Face Challenges in Timely Compliance with the EU AI Act: A Panel of Experts Weighs in on Whether Organizations Are Positioned to Meet the Requirements of the EU AI Act. MIT Sloan Management Review (June 2024)
30. Ruschemeier, H.: AI as a challenge for legal regulation–the scope of application of the artificial intelligence act proposal. In: Era Forum, vol. 23, pp. 361–376, Springer (2023)
31. Scantamburlo, T., Falcarin, P., Veneri, A., Fabris, A., Gallese, C., Billa, V., Rotolo, F., Marcuzzi, F.: Software Systems Compliance with the AI Act: Lessons Learned from an International Challenge. In: Proceedings of the 2nd International Workshop on Responsible AI Engineering, pp. 44–51 (2024)
32. Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K.: How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act. SSRN 3899991 (2021)
33. Tan, S., Taeihagh, A., Baxter, K.: The risks of machine learning systems. arXiv preprint arXiv:2204.09852 (2022)
34. Terrier, F.: No Trust without regulation! arXiv preprint arXiv:2311.06263 (2023)
35. Veale, M., Zuiderveen Borgesius, F.: Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. Computer Law Review International **22**(4), 97–112 (2021)
36. Wachter, S.: Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond. Yale Journal of Law and Technology **26**(3) (2024)
37. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly pp. xiii–xxiii (2002)
38. White, J.: Understanding the EU AI Act's Impact and Ripple Effects in the US (October 2024), URL https://www.informationweek.com/machine-learning-ai/understanding-the-eu-ai-act-s-impact-and-ripple-effects-in-the-us