ENISA Advisory Group

On the role of ENISA in cybersecurity for AI

June 2025

AUTHORS

Marta Beltrán Pardo, Ana Ferreira, Eva Fogelström, Thomas Haeberlen, Liina Kamm, Emmanuel Kessler, Wolfgang Klasen, Stephane Lenco, Matti Mantere, Ana-Maria Matejic, Roxana Radu, Bart Preneel, Luca Zampaglione

ACKNOWLEDGEMENTS

ENISA activity manager support by Apostolos Malatras
Main drafting lead by Marta Beltrán Pardo and Eva Fogelström

DISCLAIMER

The opinions expressed by the Advisory Group (AG) are not binding on the European Union Agency for Cybersecurity (ENISA) and do not represent the official position of the Agency. ENISA accepts no responsibility for any opinions or statements made by the AG.

TABLE OF CONTENTS

INTRODUCTION

The relevance of secure, resilient, and trustworthy AI is recognized by the European Commission in the AI Act[1]. Along with the implementation of the AI Act, there is also a need to increase the awareness of cybersecurity and AI, and update cybersecurity strategies with respect to AI. With the sharp uptake and easy availability of AI in society, ENISA has a role to play in providing guidance and best practice, to enhance training and build capacity, and to facilitate exchange of information on cybersecurity aspects of AI.

Cybersecurity and AI can be viewed in three main dimensions, outlined by ENISA in the report on AI cybersecurity challenges[2]: cybersecurity for AI, AI to support cybersecurity, and malicious use of AI. While all aspects are relevant, this opinion paper focuses on cybersecurity for AI, and what actions ENISA should take to enhance the security posture of AI within EU. Annex A lists some initiatives that could be explored or elaborated in future opinion papers focusing on the other two aspects.

This opinion paper recommends specific activities for ENISA, structured according to ENISA operational activities established in the Single Programming Document [3]:

ACTIVITY 1

ENISA should conduct policy monitoring to support identification of potential areas for policy development in cybersecurity for AI. ENISA should produce a practical guide outlining best practices for securing AI systems. The AG recommends increasing awareness of the varied risks of AI among policymakers. The AG suggests that ENISA emphasises a request for explainability.

ACTIVITY 2

ENISA should increase awareness while supporting the implementation of the NIS2 and the AI Act, by providing (a) an interoperable EU risk management toolbox, (b) a specific AI risk management worksheet for SMEs, and (c) supporting material for national institutions receiving notifications on AI systems under the AI Act. The AG recommends that ENISA monitor the implementation of the AI Act in different member states (MS) to identify common cybersecurity challenges with a focus on critical sectors.

ACTIVITY 3

ENISA should provide support and tools for reviewing and updating MS national cybersecurity strategies. ENISA should organise or support specialised training programs and exercises for cybersecurity professionals focusing on AI-specific threats and defence strategies. ENISA should develop a roadmap for cybersecurity education that integrates AI-related topics at various levels. The AG recommends creating and disseminating easily understandable content about AI cybersecurity risks and best practices.

[1] Artificial Intelligence Act. REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Union.*
[2] Artificial Intelligence Cybersecurity Challenges. ENISA report December 15, 2020.
[3] ENISA Single Programming Document 2025 – 2027, ENISA publication February 17, 2025.

ACTIVITY 4

ENISA should support organisations that receive AI Act notices by facilitating exchange of experiences. ENISA should create a structured process for reporting, validating, and disclosing vulnerabilities in AI systems. The AG suggests that ENISA introduces some injects related to AI in the next Cyber Europe exercise.

ACTIVITIES 5 AND 6

ENISA should support the CSIRTs Network, EU CyCLONe, European institutions, bodies and agencies (EUIBAs) and national authorities to build and enhance standard detection and situational awareness capabilities regarding AI-related cyber threats. The AG recommends creating a framework to support MS in preparing for, responding to, and recovering from large-scale cybersecurity incidents involving AI. ENISA should help MS to develop the capability to deploy essential AI systems locally.

ACTIVITY 7

ENISA should establish methods to perform evaluation to enhance trust in AI systems, products, and services. ENISA should provide AI cybersecurity baselines and metrics for assessing the security of AI systems. ENISA should advocate for AI procurement contracts and produce a set of standardised contract clauses to verify vendor compliance.

ACTIVITY 8

ENISA should monitor the AI cybersecurity market identifying dependencies among systems, products, services and vulnerabilities as well as key trends, challenges, and opportunities. ENISA should promote platforms for collaboration among AI and cybersecurity market players. ENISA should identify research gaps and engage in dialogue with international stakeholders and institutions, leveraging its position to create formal or informal research networks and formalise cooperation with relevant actors.

Many of the proposed activities will require collaboration with the AI Office due to its competence under the AI Act.

Finally, the AG would like to emphasize that supporting the security of AI systems in the EU is not something that can be solved by adding activities to a work program; the AG is not recommending a project-oriented approach but an Agency-oriented one. ENISA needs to have the skills, capabilities, and strategy to fulfil its mission in the coming years in relation to this issue.

ACTIVITY 1: SUPPORT FOR POLICY MONITORING AND DEVELOPMENT

"Bolster policy initiatives on novel or emerging areas of technology by providing technical, fact-driven and tailor-made policy analyses and recommendations. ENISA will support EU institutions and MSs on new policy initiatives through evidence-based inputs into the policy development process."

ENISA should conduct **policy monitoring** (how policies have performed against policy goals and what impact they had) to support the identification of potential areas for policy development in cybersecurity for AI, considering both technological, geopolitical and societal trends. It should also **identify gaps, overlaps, and synergies among the existing policy initiatives and those under development**. ENISA should analyse how implemented policies have affected the targeted entities and (hopefully) increased AI cybersecurity, identifying weak points and potential improvements. This analysis should be conducted in coordination with the European Commission and EU member states and should include the production of **policy recommendations, reports, papers, or opinions**. This activity should also promote dialogue with stakeholders and ensure that cybersecurity for AI is embedded across all domains of EU policies.

ENISA should produce **a practical guide outlining best practices for securing AI systems** and generate a gap analysis comparing it to EU policies (existing and under development) and EU best practices. Policy recommendations to improve the EU's approach to AI cybersecurity should be informed by the policy monitoring results mentioned before and by this **gap analysis**.

The Advisory Group (AG) recommends focusing on **increasing awareness of the varied risks of AI among policymakers**. While AI systems are information systems and, as such, have the same information security issues as regular IT systems, **extra attention needs to be directed towards questions of data visibility and data subject rights**, as the data in AI systems is often not explicitly visible. The additional **AI algorithmic vulnerabilities** (such as model poisoning, adversarial learning, prompt injection evasion attacks, information extraction attacks or denial-of-service attacks) need special attention. More broadly, the use of AI also needs to be considered against societal and ethical challenges, such as **misuse, biased models, and exploitative or addictive applications**. Furthermore, it is essential to consider the different risks affecting local and centralised models.

The AG suggests that ENISA emphasises a **request for explainability**. ENISA should stress in its policy recommendations the need to differentiate scenarios where AI is a decision-support tool and where it is a decision-maker. And the differences between risks and their potential impacts. ENISA should **raise awareness of the fallibility of AI** and stress the need for explainability in all AI systems. Furthermore, ENISA should elaborate **on the relationship between explainability in AI systems and cybersecurity**, given that a lack of explainability may affect an organisation's ability to investigate and mitigate against the impacts of an AI-system compromise. Explainable systems can be debugged and monitored more easily and lend themselves to more thorough documentation, audit, and governance.

ACTIVITY 2: CYBERSECURITY AND RESILIENCE OF CRITICAL SECTORS

"Support Member States and EU Institutions with the implementation of the NIS2. The objectives of this activity are the rapid and harmonised implementation of NIS2, to increase the maturity of NIS sectors and to ensure NIS2-aligned implementation of sectorial resilience policies, such as DORA for resilience in the finance sector and the Network code for the cybersecurity of cross-border electricity flows."

ENISA should **work on the interplay between the NIS2 and the AI Act** on risk management and securing AI systems used in critical sectors. It is not possible to do this without discussing the integration and compliance of AI models and systems with the **requirements of the AI Act**. ENISA, as part of the Advisory Forum (Article 67) to ensure the involvement of stakeholders in the implementation and application of this Regulation, can help in increasing awareness and literacy while **supporting the implementation of the AI Act** by, among others, providing guidance and recommendations on AI risk management or specific security controls. For example, cybersecurity requirements for high-risk AI systems or general-purpose AI models presenting systemic risks, AI cybersecurity metrics, benchmarks, or particular controls.

Concerning AI risk management, ENISA should provide an **interoperable EU risk management toolbox**, as well as a framework and standards[4] adapted to AI systems risk assessment, with practical guidelines for providers to harmonise the identification, validation and management of risks in **high-risk AI systems**. These must include the necessary monitoring/supervisory tools for changes that may happen over the AI system lifecycle. ENISA can help assure compliance with mandatory risk assessment requirements such as the quality and relevance of data sets used, technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy and cybersecurity.

Small and medium-sized organisations often do not have an information security management system (ISMS) nor a risk management policy in place, and it is difficult for them to identify, analyse, assess and mitigate cybersecurity and AI risks. ENISA should work on providing a specific **AI risk management worksheet for SMEs and less mature organisations.** This worksheet would provide easy access and increased awareness of the minimal required steps when adopting a system with an AI component. This could be complemented by a set of good practices that an organisation can use to identify and analyse the key cybersecurity issues of AI systems that might be relevant to them. Risk analysis and mitigation for AI systems are easier to conduct if an organisation has a risk management approach in place, but for those that do not, a simplified worksheet or tool could make the difference between support and harm from using AI systems. Moreover, the simplified worksheet could be a step towards adopting a full-scale risk management methodology for SMEs.

[4] Interoperable EU Risk Management Framework. 2022. ENISA. https://www.enisa.europa.eu/topics/risk-management

For specific security controls, and as mentioned in Recital 78 of the AI Act, the European Commission should cooperate with ENISA on issues related to the cybersecurity of AI systems. The required level of cybersecurity needs to be in line with the systems' risks and fundamental rights, as mentioned before, and **cybersecurity measures taken by the providers of high-risk AI systems** also need to consider the underlying ICT infrastructure. Suitable security controls need to be applied with the aim of providing cyber resilience to the AI system regarding attempts by unauthorised third parties to alter its use, behaviour, or performance, including AI-specific vulnerabilities such as data poisoning or adversarial attacks. Additionally, cybersecurity protection should also consider accidental model leakage, membership inference, unauthorised releases, circumvention of safety measures, and defence against cyberattacks, unauthorised access or model theft.

There is a need for clear legal harmonisation in Europe. ENISA should analyse the **cybersecurity aspects of AI in the context of relevant EU policy initiatives** (the NIS2 Directive but also the AI Act, the Cyber Resilience Act, the GDPR or IP law) to provide technical, fact-driven, and tailored cybersecurity advice and recommendations considering these policy initiatives independently but also their interplay. The desired results of this task include improved effectiveness and consistency in the implementation of EU cybersecurity policies. ENISA, together with other stakeholders of the advisory forum defined in recital 150 of the AI Act, can contribute to the synthetisation of **a grid where specific but common aspects of AI cybersecurity are merged into the requirements of the various legislations** (e.g., NIS2, GDPR, CRA, etc.). Consulting such a grid would help clearly identify the requirements that are compliant and those that fail for proper continuous auditing and correction. The AG would like to highlight here the importance of **standardised nomenclature and taxonomies within the EU**.

In addition, ENISA should provide **supporting material for national institutions receiving notifications on AI systems under the AI Act** (notified bodies), focusing on handling these notifications and which ones require specific responses. This task is vital because the AI Act introduces new obligations and procedures for AI systems, and national institutions need clear guidance on implementing them. The agency's work should focus on developing practical, actionable resources that support consistent and effective application of the AI Act across all member states concerning cybersecurity. The agency could develop specific guidance documents, checklists, templates or a catalogue of supplementary measures that national institutions can use to process and respond to notifications under the AI Act.

The AG recommends that ENISA monitor the implementation of the AI Act in different member states to **identify common cybersecurity challenges in critical sectors** and provide additional support as needed. If **simplification opportunities** around notification and reporting obligations are identified during the process, ENISA's opinion could be considered within the **digital simplification package**.

ACTIVITY 3: CAPACITY BUILDING

"Improve the capabilities of Member States, Union Institutions, bodies, and agencies, as well as, public and private stakeholders from NIS 2 Sectors. It focuses on improving stakeholders' resilience and response capabilities, enhancing their skills and behavioural change with regards to cyber hygiene, and increasing their preparedness."

ENISA should provide **support and specific tools for reviewing and updating MS national cybersecurity strategies**. The AG recommends that ENISA produce an **initial checklist of the elements to be considered in revising** these national strategies, particularly integration and dependence on AI systems for essential services. The checklist could be tested and improved through workshops and roundtables, which would also serve as a community-building function.

Some of the initiatives mentioned before (in activities 1 and 2) would help build **capacity for mitigating AI cybersecurity risks (guide with best practices, risk management toolbox, compilation of specific security controls)**. The objective should be to provide **practical technical guidelines for securing AI systems**, addressing key vulnerabilities and mitigation strategies, and clarifying how cybersecurity policies and frameworks apply to AI. A consolidated list of resources **categorised** by risk type, type of AI system or organisation would provide a quick reference for stakeholders seeking to deepen their knowledge. An **open library of use cases as examples of how to manage risk and apply security controls** could be of great help, too.

ENISA could promote or support the creation of an **AI Cybersecurity Information Sharing and Analysis Centre** focused on AI cybersecurity to facilitate the **sharing of threat intelligence, best practices, and incident response strategies** among stakeholders. This centre would serve as a central hub for collecting, analysing, and disseminating information about AI-related cyber threats, vulnerabilities, and incidents, as well as improving situational awareness and faster incident response capabilities across MS. The AG recommends building this Centre on existing threat intelligence exchange channels, to guarantee a greater and faster adoption.

ENISA should organise or support **specialised training programs and exercises for cybersecurity professionals focusing on AI-specific threats and defence strategies**. These initiatives should include how to conduct vulnerability assessments or red teaming exercises to identify weaknesses in AI systems and infrastructure, consistent with "shift left" approaches. Disseminating knowledge about both the risk identification and analysis methods, as well as the mitigation measures, will help organisations deploy AI systems more securely. Furthermore, ENISA could organise **workshops, challenges and hackathons to foster innovation and collaboration** in securing AI systems. The activities should enhance collaboration between policymakers, the technical community, and key corporate representatives to investigate better, prevent, and mitigate AI-related incidents. Another objective could be creating **a community/group of experts focused on addressing AI security challenges**.

In general, ENISA should work on **improving AI cybersecurity literacy and skills**. Research is needed **on the necessary competencies to securely use AI systems or on how to secure AI systems** and how to keep doing this while the environment and technology change quickly.

The AG recommends **creating and disseminating easily understandable (for the general public) content about AI cybersecurity risks and best practices** through various media channels. ENISA should support other institutions in **promoting AI literacy**, public awareness, and understanding of the

benefits, risks, safeguards, and rights and obligations related to the use of AI systems. **The Awareness Raising in a Box (AR-in-a-BOX) package should be reviewed and updated to meet this objective.**

ENISA should develop a structured roadmap for cybersecurity education that integrates AI-related topics at various levels, from primary and secondary education to vocational training and higher education. The roadmap should identify key skills and competencies needed for the AI-driven cybersecurity landscape and outline pathways for individuals to acquire these skills. Considering the performed analysis, the European Cybersecurity Skills Framework (ECSF) should be reviewed and updated. Links to global initiatives such as the European Digital Education Action Plan or the AI Continent Action Plan should be established, too.

This exercise will also help to understand and devise toolsets to be adopted in various contexts and for different age ranges. For example, such toolsets can help teachers educate younger students in both subjects, as well as increase the awareness and literacy of non-professionals and the population in general in those two areas—cybersecurity and AI—that impact their everyday activity and interaction with technology now and more so in the future.

ACTIVITY 4: ENABLING OPERATIONAL COOPERATION

"Support operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities. The main goal of the activity is to provide support and assistance in order to ensure the efficient functioning of EU operational networks and cyber crisis management mechanisms."

Organisations can expect to start receiving notices from authorities, as the different chapters of the AI Act enter into application. As of the time this opinion paper is written, only Chapter I General Provisions and Chapter 2 Prohibited AI Practices are in application. These notices might indicate a possible violation of the AI Act, an Investigation & Audit notice or a Warning among others.

ENISA should **support organisations that receive AI Act notices by organising meetings, round tables, or workshops** where they can exchange experiences, learn from each other, and plan solutions to address the notices received.

ENISA should create (or integrate in the existing one) **a structured process for reporting, validating, and disclosing vulnerabilities in AI systems**. This process should outline all stakeholders' roles and responsibilities, ensuring vulnerabilities are addressed promptly and effectively. The process should include guidelines on responsible disclosure timelines, communication protocols, and remediation steps. ENISA should create and disseminate **specific guidelines for remediating and mitigating AI vulnerabilities, providing actionable steps for vendors, developers and users to address identified weaknesses**. These guidelines should cover a wide range of vulnerabilities and complement existing resources considering the extended attack surface, the complexity of the supply chains, the data dependency, etc. ENISA should **foster collaboration and information sharing** among stakeholders to enhance awareness and response to AI vulnerabilities. This includes establishing **formal and informal communication channels and participating in industry forums**, always encouraging the development of secure AI systems.

The use of AI is spreading to all sectors, and many organisations are starting to delegate some decisions and automation tasks to AI systems. Therefore, the AG suggests that ENISA **introduce some injects related to AI in the next Cyber Europe exercise**. Cyber Europe could include some injects in which an attacker or a malicious user is able to manipulate an AI model to make different decisions at a critical level (such as energy, medical or financial), automate attacks using AI models or exploit AI models in a supply chain scenario to modify the behaviour of a security/critical system at the vendor level, affecting all the customers.

The goal would be to develop some scenario where the participants have to deal with an AI-related incident and not only to include AI in the list of potential threats but also to encourage the industry to develop or **adapt the incident response and business continuity/recovery plans considering the AI**.

ACTIVITY 5: PROVIDE EFFECTIVE OPERATIONAL COOPERATION THROUGH SITUATIONAL AWARENESS &

ACTIVITY 6: PROVIDE SERVICES FOR OPERATIONAL ASSISTANCE AND SUPPORT

Activity 5 "Contribute to cooperative preparedness and responses at the level of the Union and Member States through data driven analyses of threats and risks, operational and strategic recommendations based on the collection of incidents, information on vulnerabilities and threats in order to contribute to the Union's common situational awareness."

Activity 6 "Contribute to the further development of capablilities to prepare and respond at the level of the Union and Member States for large-scale cross-border incidents or crises related to cybersecurity through the implementation and delivery of ex-ante and ex-post services."

ENISA should support the CSIRTs Network, EU CyCLONe, EUIBAs and national authorities to build and enhance **standard detection and situational awareness capabilities regarding AI-related cyber threats**. These capabilities should focus on monitoring AI systems, detecting anomalies, and sharing threat intelligence. The **AI Cybersecurity Information Sharing and Analysis Centre** mentioned in Activity 3 may have an essential role in this activity, making possible shared situational awareness, increased common understanding and timely access to information regarding the latest threats, incidents and vulnerabilities.

ENISA should promote the organisation of coordinated testing exercises to evaluate the preparedness and resilience of specific AI systems against cyberattacks. These exercises should involve various sectors and simulate real-world attack scenarios. ENISA should be consulted in **identifying sectors/subsectors for which coordinated preparedness testing should be conducted**. ENISA may develop **common risk scenarios and methodologies** for these coordinated testing exercises. These scenarios should be based on current threat intelligence and address AI-specific vulnerabilities.

ENISA should support MS when responding to AI-related incidents. The AG recommends creating **a framework to support MS in preparing for, responding to, and recovering from large-scale cybersecurity incidents involving AI**. This mechanism should include preparedness measures, requests for support at different levels and mutual assistance protocols. It should also define the criteria for declaring an “AI cyber emergency” (given the scale, the impact on essential services, etc.) and activating different response/recovery protocols.

The AG recommends ENISA to **create detailed, standardised protocols for recovering AI systems after a cyber incident**. These protocols should include steps for data restoration, model retraining, and vulnerability patching. They should also address the unique challenges posed by AI systems, such as ensuring that retrained models are free from biases or backdoors introduced during the attack.

ENISA should help MS to **develop the capability to deploy essential AI systems locally** (e.g. within national data centres or secure facilities) during a crisis, ensuring the continuity of critical services even if external or cloud-based AI infrastructure is compromised. This includes identifying key AI applications vital for national security, public safety, and economic stability and creating redundant, locally hosted versions. A good example of such a system would be the GPT@JRC system running at the Joint Research Centre of the European Commission.

ACTIVITY 7[5]: DEVELOPMENT AND MAINTENANCE OF TECHNICAL GUIDANCE ON EVALUATION PROCESSES

ENISA should focus on **establishing methods to perform evaluation processes to enhance trust in AI systems, products, and services**. AI systems are not always complete, predictable and repeatable. Therefore, an evaluation process for AI shall be understood as a living system that shall include the principles of "**Secure by Design, Secure by Default, Secure in Operations" and be risk-based**.

ENISA should provide **AI cybersecurity baselines**, defining minimum security standards (practices and controls) for AI systems, products, and services used in different contexts. These baselines will serve as a reference point for evaluating AI cybersecurity. The desired result is a clear and consistent understanding of what constitutes "secure AI" across different sectors and applications. ENISA should **publish different baselines (per type of AI system, per type of organisation, per application domain, etc.), along with tools and templates for assessing gaps or compliance**. Such baselines should be derived ideally from normalisation bodies and standards or overseen by a private third party such as the EuroNCAP group for automotive. The EU may require those baseline assessments to be performed to access the EU market or define a minimum acceptable result level.

Regarding these baselines, ENISA should define **objectives and quantifiable metrics for assessing the security of AI systems from different points of view**. The AG recommends creating **benchmarks to measure these figures** for different AI systems. In addition, evaluation tools and reporting templates should be provided. During its market life, technology will evolve, and vulnerabilities may emerge. A regulatory body may operate like EASA in aviation to mandate changes to an existing AI system, restrict them from the market until a satisfactory resolution, and provide public lessons learned to feed the baselines. This implies that every AI system operating in the EU must have a declared "responsible" owner who shall be contacted for those measures. Such an EU oversight AI body may be granted **regular security audit capabilities** or have a mandate to respond to inquiries from MS or the European Commission on specific topics. ENISA could work on materialising this type of concept, providing the required technical guidance.

Finally, ENISA should advocate for **AI procurement contracts, including specific requirements for AI security**. Contracts should ensure that AI vendors demonstrate compliance with the established AI security baselines and provide evidence of ongoing monitoring and improvement (for example, using the proposed benchmarks). The desired result is that AI systems acquired by the MS governments meet the highest standards of security and reliability. ENISA should produce **a set of standardised contract clauses related to AI security and the process for verifying vendor compliance**.

[5] Activity 7 in the ENISA Single Programming Document 2025-2027 is “Supporting Development and maintenance of EU cybersecurity certification framework”. Since under Article 21(5) of the Cybersecurity Act, the AG shall advise ENISA in respect of the performance of the tasks of the Agency, except for those provided for in Title III of the Cybersecurity Act (which concerns the cybersecurity certification framework), the AG has decided to provide recommendations on a different activity “Development and maintenance of technical guidance on evaluation processes”, that is in its scope and related to the original activity 7.

ACTIVITY 8: SUPPORTING EUROPEAN CYBERSECURITY MARKET, RESEARCH & DEVELOPMENT AND INDUSTRY

> ***"Foster the cybersecurity market for products and services in the European Union along with the development of the cybersecurity industry and services, in particular for SMEs and start-ups, to reduce dependence from outside and increase the capacity of the Union and to reinforce supply chains to the benefit of the internal market."***

The complexity of the AI supply chains has been mentioned before in this opinion paper. ENISA should perform **regular analyses of the AI cybersecurity market to monitor, collect and identify dependencies among systems, products, services and vulnerabilities**. ENISA should promote platforms for **collaboration among AI and cybersecurity market players**, improving visibility in the digital single market. This involves organizing workshops, conferences, and online forums where vendors, innovators and researchers can share knowledge, exchange ideas, and forge partnerships. The desired result is enhanced innovation and the development of more effective AI cybersecurity solutions.

ENISA should also perform regular in-depth **analyses of the AI cybersecurity market** to identify key trends, challenges, and opportunities. The analysis should cover the demand side (e.g. needs and preferences of organisations seeking AI cybersecurity solutions) and the supply side (e.g. capabilities and offerings of AI cybersecurity vendors). An **annual report detailing specific market trends, competitive landscapes, and emerging technologies is the desired result**. ENISA could conduct **regular surveys to assess the satisfaction levels of essential stakeholders with the available AI cybersecurity solutions**. The surveys should gather feedback on factors such as product effectiveness, ease of use, customer support, or pricing. This would help determine actual needs and identify areas for improvement. Furthermore, ENISA should **monitor standardisation developments that have implications for AI cybersecurity**.

ENISA can actively enhance knowledge about emerging challenges and opportunities by regularly conducting **horizon scanning exercises and research briefs** on emerging threats and vulnerabilities specific to AI systems. The latter could be developed in partnership with European academic institutions and be featured in **shorter formats** (blogs, videos, podcasts, etc.) to increase accessibility and reach. Moreover, ENISA should consider ways to distribute information about new AI-related threats or AI security innovations in real time so it can become actionable on the ground as soon as it is available. In the long run, ENISA should support **integrating AI analysis as part of broader threat and risk analysis and security design, which should be built into all systems and processes.**

ENISA should organise workshops where experts from various fields come together to develop **plausible scenarios for the future of AI cybersecurity** (foresight exercises). These scenarios should consider a range of possibilities, from optimistic to pessimistic, and explore the potential implications for the agency's mission and operations. The desired result is improved readiness for various future

scenarios and identifying robust strategies that perform well across different contexts. The AG suggests publishing detailed scenario narratives, strategic recommendations, and contingency plans.

ENISA should identify **research gaps** to help identify current and future needs and promote the definition of a strategy to encourage research of key areas. The AG recommends that ENISA adopt an active role in deciding **where advances beyond the state-of-the-art are required**. ENISA could scan for emerging technological, regulatory and societal trends impacting AI cybersecurity to determine R&I priorities. This process should involve **regularly consulting** with user groups, projects (especially EU-funded projects), researchers, universities, industry, start-ups, and digital innovation hubs to consolidate information and identify gaps, challenges, and opportunities in R&I. ENISA should also systematically **use statutory bodies** such as the National Liaison Officers (NLO) Network and the ENISA Advisory Group, as well as groups like the Stakeholder Cybersecurity Certification Group (SCCG) or expert groups created under EU law to gather meaningful and up-to-date input.

Furthermore, ENISA should **engage in dialogue with other international stakeholders and institutions, leveraging its position to create formal or informal research networks**. The agency can promote different forums for dialogue to foster knowledge sharing in both directions: **gathering information to determine the most pressing needs and sharing information so that researchers know the established priorities, and possibilities for cooperation and funding**.

ENISA should formalise **structured cooperation** with the European Commission's Joint Research Centre, the European Cybersecurity Competence Centre or the European AI Office to **coordinate research initiatives and provide strategic guidelines or directions to the EU agenda on AI cybersecurity research**: in which specific areas it would be interesting to conduct or fund research, and the priorities of these areas. Possible collaborations with current and future EU Networks of Excellence for AI cybersecurity (e.g., the EU AI & Robotics NoEs community) should be considered.

Ensuring cybersecurity considerations in various EU-funded actions that utilize AI systems or engage in related R&I is paramount. ENISA should consider **providing advice and support to the different EU workgroups responsible for establishing evaluation criteria for such activities and relevant work plans**. Such advice should take into account not only relevant EU regulations and directives but also industry best practices and, in general, reference descriptive sources. As a specific example, this support could be realized by helping define **the evaluation sub-criterion of "AI robustness",** currently a common concept for many evaluations of applications for EU-funded projects (e.g., Horizon Europe, Digital Europe Programme)

While cybersecurity of any AI systems utilized in EU-funded projects should be ensured, a balance should be struck so as not to introduce undue barriers to innovative use of AI technologies. Global differences in funding AI-related work should be considered carefully so as not to de facto to introduce further constraints that harm the competitiveness of EU-based entities.

CONCLUSIONS

Today's pervasive availability and use of AI needs to be balanced with measures to understand risks, to address cybersecurity and privacy of AI, to ensure transparency and resilience of AI. This opinion paper outlines actions for ENISA to support this global objective and to define a long-term strategy.

Such actions include assisting in policy development on cybersecurity for AI, increasing awareness through toolboxes and supporting material, support in reviewing and updating MS national strategies, facilitating exchange of experiences, and adding cybersecurity aspects of AI to cybersecurity exercises. Further actions include establishing methods for evaluation to enhance trust in AI systems, products, and services, analysis of the AI cybersecurity market, and a roadmap for education and research.

The AG would like to conclude by emphasizing the need to collaborate with the AI Office in many of the proposed activities due to its competences under the AI Act. The AI Office is tasked with developing Union expertise and capabilities in the field of AI and contributing to the implementation of Union law on AI, therefore, many activities related to cybersecurity for AI executed by a European institution will require some degree of cooperation or coordination with this Office which will have to be established on a case-by-case basis.

ANNEX A

Needs detected but not developed in this paper because they are out of scope (cybersecurity for AI):

AI TO SUPPORT CYBERSECURITY:

1. Review existing EU policy on usage of AI systems applied to cybersecurity and propose amendments, if needed, to leverage AI in cybersecurity (e.g., allow the use in blue teaming and red teaming).

2. Provide use cases, practical examples, technical guides on how to develop and deploy cybersecurity systems using AI in compliance with the AI Act.

3. Organise workshops/hackatons for developing/designing AI tools to support cybersecurity tasks, both in the blue and red team's sides. As in the case of Cybersecurity of AI, these events can be used to build a community of experts and developers.

4. Develop guidelines and best practices for integrating AI into cybersecurity operational cooperation, considering specific use cases. This could encompass recommendations on data quality, algorithm selection, model training, or performance evaluation for each case.

5. Facilitate or promote the development and adoption of AI-powered cybersecurity tools and platforms that are reliable and secure. This could involve establishing testing and evaluation criteria or frameworks or supporting the development of open-source/community-driven AI security tools.

6. Provide very specific recommendations: list of AI systems/tools to use? Or AI systems/tools to avoid?

7. Build/provide test datasets for these applications. Data from all hackathons and exercises should be made available as a resource for researchers and the cybersecurity industry.

8. Explore possibilities of sharing (e.g. data, tools) to improve cybersecurity of EU: AI for good.

9. Collaborate with EU-allies on data-driven (AI-driven) cybersecurity.

10. Promote the development of AI models maintained by MS to support the national CSIRTs in responding to cyber incidents more efficiently.

11. Explore the possibility to leverage AI for pro-active preparedness and response (adding AI to existing initiatives?).

12. Promote research and development in AI for cybersecurity, focusing on areas such as threat intelligence, vulnerability analysis, malware detection, or incident response. This could involve advising about the funding of research projects, helping to establish collaborative platforms, or fostering partnerships between academia, industry, and different agencies.

13. Identify and evaluate opportunities on the market for using AI for cybersecurity: could be tools for analysing/monitoring threat environments, or use of AI methods for security-by-design.

MALICIOUS USE OF AI:

14. Create awareness of how AI can be used to serve the needs of people with a certain agenda. AI as a threat deserves more attention: AI to threaten critical infrastructure, public opinion, alter election results, etc.

15. Conduct threat modeling or risk assessments to identify and analyze potential attack vectors and vulnerabilities arising from the malicious use of AI. This should cover a wide range of attack scenarios, including AI-powered malware or automated social engineering attacks, to mention only a couple of examples.

16. Support situational awareness by maintaining a birds-eye view of observed cases where AI has been a significant factor in either attempted or successful cyberattack.

17. Clarify the terminology, e.g. when AI is used as a tool for “cyberattack”. Is it relevant to cybersecurity when deep fakes are used to mislead the general public? Is this actually even a case of cyberattack, if so, how to classify it? If just having an AI generate the deep fake means it is “cyberattack”, are we on a slippery slope? (consider e.g. classic video manipulation and how those should be classified). When AI is used to carry out cyberattacks, is it actually of material importance that AI was utilized? If so, why? Etc.

18. Develop and disseminate guidance and best practices for defending against AI-powered cyberattacks, including strategies for detecting, responding to, and recovering from such attacks.

19. Collaborate with international partners and organizations to share intelligence and best practices on mitigating AI-driven threats. This could involve participating in joint exercises or organizing them, developing early warning systems, and promoting information exchange on emerging threats and vulnerabilities.