Artificial Intelligence Threat Reporting and Incident Response System

D8.7 Report on Policy Recommendations

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	D8.7
Deliverable Due Date:	31/8/2024
Deliverable Submission Date:	29/8/2024
Deliverable Version:	v1.0
Main author(s) and Organisation:	ECSO, CyberEthics Lab (CEL)
Work Package:	WP8 – Dissemination, Communication and Exploitation of Results
Task:	T8.4 Policy recommendation and standardisation
Dissemination Level:	PU: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Quality Control

	Name	Organisation	Date
Editor	Cristian Michael Tracci	ECSO	27/08/2024
Peer Review 1	Sotirios Spantideas	KEMEA	09/08/2024
Peer Review 2	Lorena Volpini	CEL	21/08/2024
Submitted by (Project Coordinator)	Gonçalo Cadete	INOV	29/08/2024

Contributors

Organisation
CEL
ECSO

Document History

Version	Date	Modification	Partner
v0.1	09/07/2024	Initial draft	Luca Mattei (CEL)
v0.2	31/07/2024	Full draft	Cristian Michael Tracci. Roberto Cascella (ECSO)
v0.3	27/08/2024	Addressing reviewers' comments	Cristian Michael Tracci. Roberto Cascella (ECSO)
v1.0	29/08/2024	Final editing	Gonçalo Cadete

Legal Disclaimer

IRIS is an EU project funded by the Horizon 2020 research and innovation programme under grant agreement No 101021727. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The IRIS Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
GDPR	General Data Protection Regulation
AI	Artificial Intelligence
IoT	Internet of Things
EU	European Union
Art. 29 WP	Article 29 Working Party
ICO	Information Commissioner’s Office
EPRS	European Parliamentary Research Service

1 INTRODUCTION

1.1 Project Introduction

As existing and emerging smart cities continue to expand their IoT and AI-enabled platforms, this introduces novel and complex dimensions to the threat intelligence landscape linked with identifying, responding, and sharing data related to attack vectors, based on emerging IoT and AI technologies.

IRIS's vision is to integrate and demonstrate a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding to and sharing information regarding threats & vulnerabilities of IoT and AI-driven ICT systems. To achieve this, IRIS brings together experts in cybersecurity, IoT, AI explainability, automated threat detection, response, and recovery.

IRIS aims to help European CERTs/CSIRTs minimise the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

The IRIS platform was demonstrated and validated on 3 highly realistic environments with the engagement of 3 smart cities (in Helsinki, Tallinn, and Barcelona) along with the involvement of national CERTs/CSIRTs, cybersecurity authorities, and other stakeholders.

The project duration extends from September 2021 to August 2024.

1.2 Deliverable Purpose

This deliverable aims to consolidate the key observations drawn throughout the project and offer policy recommendations for the future. It focuses on two areas: artificial intelligence and cybersecurity.

The recommendations are tailored to address multiple policy levels, including organizational, national, and EU-wide frameworks. At the organizational level, the focus is on ensuring compliance with relevant regulations, such as the AI Act and GDPR. At the national level, the recommendations highlight the need for coherent policies that align with national interests while integrating with broader EU directive. At the EU level, the emphasis is placed on harmonizing policies across member states to promote a unified approach to AI and cybersecurity challenges, like with the Cyber Solidarity Act.

With these different levels of policy, the deliverable aims to provide actionable guidance that is relevant to diverse stakeholders, ensuring that the insights from the project are effectively translated into impactful policies that drive compliance, innovation, and security across the board.

The activities on standardization are reported in Deliverable D8.5.

2 AI AND PRIVACY RECOMMENDATIONS

The IRIS project considered since its inception that the collaboration between CERTs/CSIRTs is essential for protecting the European Union from AI and IoT cyber threats. To this end, IRIS engages with this challenge by testing its innovative solution in three existing smart city environments: Helsinki, Tallinn, and Barcelona. IRIS's solid consortium composition aims to deliver improvements to the European cybersecurity ecosystem through the successful adoption of the IRIS's innovative features.

In order to ensure the effective and widespread deployment of IRIS results, the present report provides considerations collected during the project on policy recommendations. The activities on standardization are reported in Deliverable D8.5. This is a fundamental step to guarantee the adoption and the interoperability of the technologies developed by IRIS Project. For this reason, with this contribution, CEL provides 9 policy recommendations extracted from some of the most important frameworks from the perspective of privacy, data protection, and AI regulation. These distinct but intertwined dimensions laid the foundation for a methodology which identifies the challenges and concerns, as well as countermeasures, to be considered for the development, in order to be compliant with the current and evolving EU regulatory frameworks. This activity includes the analysis of a well-established framework such as the General Data Protection Regulation, but also the recent cross-cutting regulation on Artificial Intelligence, the AI Act.

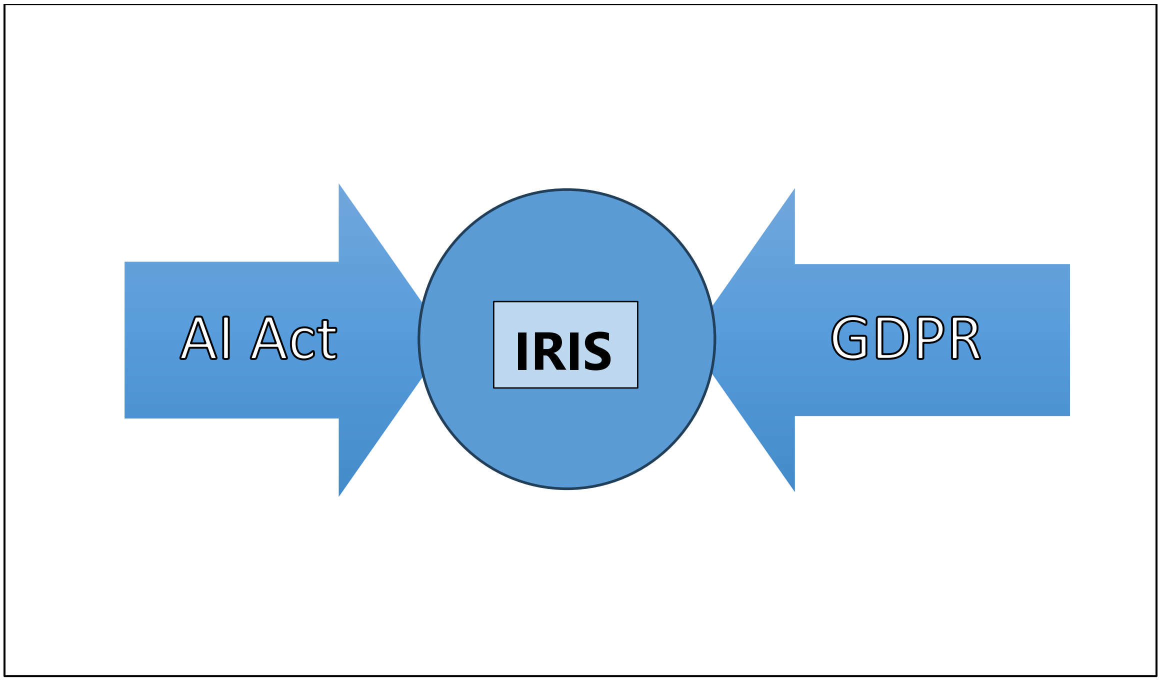

Figure 1 The need to plan for compliance with GDPR and the AI Act

2.1 The AI Act

The uptake of artificial intelligence (AI) systems has a strong potential to bring societal benefits, economic growth and enhance EU innovation and global competitiveness. At the same time, it is commonly acknowledged that the specific characteristics of certain AI systems raise some concerns especially with regard to safety, security and fundamental rights protection. Against this backdrop, the European Commission unveiled a proposal for a new artificial intelligence act (AI Act) in April 2021. The AI act has been formally adopted by Parliament in its March 2024 plenary session (with a corrigendum issued in April 2024) and the Council endorsed the final text in May 2024. The AI Act will soon enter into force, i.e. 20 days after its publication in the EU's Official Journal, and shall apply from 2 August 2026, although some parts will be applicable sooner[1].

2.1.1 The AI definition

An aspect of the AI Act that has been the subject of great contention during the legislative process is the definition of AI itself. This aspect was not easy to settle, as there are several legal, technical and academic sources that define artificial intelligence using different terms. In the end, even the definition pushed forward by the European Commission in its 2021 proposal was modified in the definitive version of 2024. Therefore, according to Art. 3(1) of the AI Act:

AI System
[A] machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

This is the first step for understanding whether the AI Act applies to a particular technology. In the case of IRIS, partners developing technologies that fall under this definition need to pay close attention to this new regulation and how it will be applied in the coming years. This is a necessary step in order to obtain CE marking and access the European market.

2.1.2 The objective scope

Extensive as it is, the AI Act does not apply to all domains. In fact, the Art. 2 of this legal text establishes several objective exemptions to its applications. There is a whole range of domains toward which the AI Act will not take effect. For instance, according to Art. 2(3), the AI act is not applicable to an AI system which is "placed on the market, put into service, or used with or without modification for military, defence or national security purposes", or even if its output is used in the Union for the same reasons. Interestingly, Art. 2(4) also

[1] https://eur-lex.europa.eu/eli/reg/2024/1689/oj

states that the AI Act does not apply to "AI systems or AI models" designed for the "sole purpose of scientific research and development".

Finally, this regulation also does not apply to AI systems that fall under the definition of open-source. This is an important disposition for IRIS, as open-source is an important asset for the project. However, it should be kept in mind that there are several requirements for accessing the exemption to the AI Act related to open-source. According to Recital 103:

AI Act, Recital 103
Free and open-source AI components cover the software and data, including models and general-purpose AI models, tools, services or processes of an AI system. Free and open-source AI components can be provided through different channels, including their development on open repositories. For the purposes of this Regulation, **AI components that are provided against a price or otherwise monetised**, including through the provision of technical support or other services, including through a software platform, related to the AI component, or the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, with the exception of transactions between microenterprises, **should not benefit from the exceptions provided to free and open-source AI components**. The fact of making AI components available through open repositories should not, in itself, constitute a monetisation.

2.1.3 The risk classification

This piece of legislation contains extensive, cross-cutting regulations across the AI pipeline for the purpose of ensuring the safety of products adopting this technology. Its approach is risk-based and divides the AI systems under its scope in different risk classes. The highest one is "Prohibited AI practices" expressed in Art. 5, while the second is "High-risk AI systems", enshrined in Art. 6 and Annex III. The full applicability of the entire legal framework will not occur in the immediate future, as it will be subject to gradual adoption. Table 1 below summarizes the main steps that the AI Act still needs to address.

Table 1 Summary roadmap to the full entry into force of the AI Act

Time lapse after entry into force	Effects	Details
6 months	• Prohibitions on unacceptable risk AI, as listed in Art. 5.	• E.g. The placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness

Time lapse after entry into force	Effects	Details
12 months	• Appointment of Member States competent authorities; • Annual review of the Commission on the list of prohibited AI.	//
18 months	• Commission implementing act on post-market monitoring.	//
24 months	• Obligations on high-risk AI systems, as listed in Annex III.	For instance: • Biometrics; • Critical infrastructure; • Education; • Employment; • Access to essential public services.
36 months	• Obligations on high-risk AI systems, as expressed in Art. 6(1) of the AI Act.	• E.g. the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I.

It is clear from this summary table that the obligations for those involved in the AI pipeline are bound to increase over time. In particular, the compliance of providers of AI systems that can be defined as 'high-risk' will need to be carefully considered, especially for what concerns the accountability duties of providers regarding the Quality Management System (Art. 17) and Information Keeping (Art. 18). For these reasons, it will be necessary to determine whether future IRIS technology deployments fall into this category.

To sum up, the AI Act is a regulation that will have a great impact in the European tech market. Therefore, it is necessary for all actors involved in this business to take due account of it. At the time of writing this contribution, the AI Act has not yet been published in the Official Journal of the European Union, but this will most likely happen very soon, and from that point on it will slowly begin to take effect. At this stage of technological and regulatory evolution, it is appropriate to begin defining a strategy for IRIS compliance. The goal is to ensure that compliance with the AI Act can be taken into account in the design and implementation of IRIS itself. Therefore, the following recommendations are made.

Table 2 Recommendations related to the AI Act

Recommendations	Description
AI Legal Recommendation 1	What is AI and what is not is not up to debate from the regulatory perspective of the AI Act. It should be avoided to engage in debates about what constitutes AI from a general or technical perspective. Instead, the focus should be on the regulatory definition provided in the AI Act. An AI Classification assessment should be conducted regarding IRIS platform, or some of its components, to understand if they fall under the definition of AI provided in Art. 3(1).
AI Legal Recommendation 2	There are several exceptions to the objective scope of the AI Act. In particular, it should be analysed whether IRIS, or some of its components, fall under the open-source exception described in 2.1.3.
AI Legal Recommendation 3	The AI Act is a risk-based legal framework. As such, it is divided into 4 classes of risk (minimal risk, limited risk, high risk or unacceptable risk). It should be analysed under which one of them IRIS, or some of its components, falls into. To this end, several factors must be taken into account: as stated in section 1.1. of the DoA (Part A), IRIS should support "CERTs/CSIRTs to collaboratively protect critical infrastructures." This could affect the AI Act classification, since, as shown in the Table 1, critical infrastructure is one of the domains that fall under "High-Risk AI" classification.
AI Legal Recommendation 4	Given the fact that the AI Act will come into effect slowly over the course of a few years, it is necessary to allocate time and

Recommendations	Description
	resources to monitor the developments behind this legislation. In particular, one must continue to monitor the clarification and guidance activities that will be issued by the AI Office and the European Commission.
AI Legal Recommendation 5	In close connection to "AI Legal Recommendation 3", a strategy for complying with the AI Act must be promptly established. As such, particular emphasis must be given to accountability and components such as the Data Protection and Accountability (D7.5) must be incorporated within coherent and well-organised compliance framework.

2.2 The GDPR

Unlike the AI Act, the GDPR is a framework that has been in place for several years. Nonetheless, it is worth reiterating its discipline, also for its repercussion on AI governance. This section provides data protection general principles, in accordance with best practices, rules, and recommendations, including documents such as:

- The Article 29 Working Party (Art. 29 WP) Guidelines on Data Protection Impact Assessment;
- The study of the European Parliamentary Research Service (EPRS) on "The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence";
- The Information Commissioner's Office Checklist on data protection principles;

The data protection principles are listed below and described in Table 3, together with their requirements in accordance with ICO's Checklist:

- Lawfulness;
- Fairness;
- Transparency;
- Purpose Limitation;
- Data Minimisation;
- Accuracy;
- Storage Limitation;
- Security;
- Accountability.

Table 3 Description of data protection principles

Data Protection Principles description
Lawfulness
The data processing must be grounded in a legal basis (e.g. consent, Art. 6(1), GDPR).
□ An appropriate lawful basis (or bases) for data processing is identified -.
□ If the data processing involves special categories data (Art. 9, GDPR) or criminal offence da-ta, a special condition for processing this type of data is identified.
□ Personal data are not employed for anything unlawful.
Fairness
The personal data processing must not infringe in unreasonable manner the fundamental rights and freedoms of data subject.
□ How the processing may affect the individuals concerned is considered and justifications for any adverse impact are provided.
□ People's data are handled in ways they would reasonably expect, or is explained why any unexpected processing is justified.
□ People are not deceived or mislead when their personal data are collected.
Transparency
According to Recital 58 of the GDPR, transparency means that "any information addressed to the public or to the data subject [must] be concise, easily accessible and easy to understand", employing "plain" and "clear" language.
□ Compliance with honesty and openness with the transparency obligations of the right to be informed (e.g. information and communication regarding the processing of personal data must be easily accessible and easy to understand, and that clear and plain language be used.
□ the data subject receives information on the identity of controllers and the purposes of the processing of personal data as well as further information useful to ensure fair and transparent data processing.
Purpose limitation
A purpose (or purposes) for processing must be clearly identified.:
□ The purpose(s) is documented.
□ Details of the purpose(s) shall be included in the privacy notice to individuals.
□ The processing shall be periodically reviewed and, where necessary, the documentation and privacy notices to individuals shall be updated. –
□ Where personal data is used for a new purpose, other than a legal obligation or a function specified by law, and where it is compatible with the original purpose, specific consent will be obtained for the new purpose.
Data minimization
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Data may only be processed if they are necessary to achieve the purposes mentioned above.
□ Only personal data that is actually necessary for the purpose(s) will be collected.
□ The personal data collected is sufficient to properly fulfil those purposes

Data Protection Principles description
□ The personal data collected is periodically reviewed and any data that is no longer needed is deleted.
Accuracy
Personal data must be accurate, and, where necessary, kept up to date. Every reasonable step is taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay. This means that:
□ The accuracy of any personal data created must be ensured.
□ Appropriate processes to check the accuracy of the data collected are put in place, and the source of that data is recorded.
□ A process to identify when is necessary to update the data to properly fulfil the purpose(s) is defined.
□ If it is necessary to keep a record of a mistake, it is clearly identified as a mistake.
□ The records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.
□ The individual's right to rectification is ensured and any challenges to the accuracy of the personal data are carefully considered.
□ As a matter of good practice, a note of any challenges to the accuracy of the personal data is kept.
Storage Limitation
Based on this principle, a Partner shall not retain personal data for longer than is necessary for the purposes for which the personal data is processed, shall justify why it retains personal data, and shall have a data retention policy for deleting or anonymising data. Accordingly, the data controller must establish/ensure:
□ Why personal data is held and why it is needed.
□ How long personal data is kept is carefully considered and can be justified.
□ A policy with standard retention periods (where possible and in line with documentation requirements) is developed and maintained.
□ That personal data is regularly reviewed and deleted or anonymised when no longer required.
□ An appropriate process is in place to comply with individuals' requests for deletion under the 'right to be forgotten'.
□ Any personal data held for public interest archiving, scientific or historical research or statistical purposes is clearly identified.
Security ('Integrity and confidentiality')
Appropriate technical and organisational measures must secure Personal Data against unauthorised or unlawful processing, accidental loss, destruction or damage.
Accountability
GDPR integrates accountability as a principle that requires that organisations put in place appropriate technical and organisational measures and demonstrate what they did and its effectiveness when requested, as well as demonstrate that they are compliant with the law. A good step toward compliance with this principle is to perform a Data

Data Protection Principles description
Protection Impact Assessment (DPIA), though this procedure is not always mandatory, as clarified by the Art. 29 WP Guidelines on Data Protection Impact Assessment.

As already mentioned, these principles are applicable also to the AI field. The AI-based solutions process vast amount of data, and sometimes even personal data. This information gives opportunities, but also raise risks to the privacy and data protection of the individuals. Therefore, on the basis of the data protection principles just described, the following recommendations are enunciated.

Table 4 Data protection recommendation

Recommendations	Description
Data Protection Recommendation 1	It must be determined with clarity whether the AI solution processes (or might process) personal data. This means that we need to analyse the data flow characteristics to see if they meet the definition of personal data in Art. 4(1) of the GDPR.
Data Protection Recommendation 2	There is a clear difference between: 1. the idea of transparent and explainable AI; and 2. the principle of transparency, as described in the Recital 58 of the GDPR. The first "involves building a 'scientific' model of the functioning of an AI system" (EPRS, 2020, p. 44). Instead, the second as pointed by the EPRS in its report, involves proactive conducts ordered to provide sufficient concise, accessible and understandable information about data processing to the people involved, such as the public and the data subject. When developing and deploying AI systems, it is recommendable to ensure that both aspects are addressed: provide clear, accessible information to users and data subjects about relevant issues, while also working towards a deeper, technical understanding of the AI's functioning for scientific and developmental purposes.

Recommendations	Description
Data Protection Recommendation 3	In order to enable compliance with data protection principles, these must be taken into account from the onset. This approach is also called in the GDPR (Art. 25) data protection by design and data protection by default. It means that data protection principles must be promptly incorporated into the design of the solution, since the development stage. This may entail, not exhaustively: • establishing default settings in AI systems that automatically ensure the highest level of data protection; • integrating Data Protection Principles from inception, e.g. by implementing a mandatory protocol ensuring their incorporation from the earliest stages of AI system conceptualisation and development, and • creating a checklist of data protection requirements to be addressed at each phase of the AI development lifecycle.
Data Protection Recommendation 4	Whenever possible, prioritise anonymisation and pseudonymisation to facilitate the compliance with GDPR. To do so it is recommendable to put in place methodologies aimed at lowering the data processing in AI data processing activities Implement anonymisation and pseudonymisation techniques wherever possible in AI data processing activities. These are key strategies to lower data processing risk levels in AI systems.

3 Relevant European Cybersecurity Policies: NIS2 Directive and Cyber Solidarity Act

3.1 Introduction

Seemingly new technologies like AI experience a growing commercialization today, however, neither the technologies themselves nor their foundational cybersecurity challenges are new. They have existed for the better part of the last 30 years. Similarly, the information-sharing sub-field has undergone a similar trend. The earliest references to policies supporting information-sharing initiatives (e.g., ISACs) date back more than 20 years. Yet, despite numerous initiatives and efforts, information sharing continues to face foundational challenges.

Some improvements might be on the horizon thought. The European institutions have undertaken some important policy initiatives lately, aimed to further shape information sharing among various cybersecurity stakeholders. While several projects, organizations, and ad-hoc initiatives exist, references to information sharing can be recalled primarily in the two major EU cybersecurity policies: the NIS2 Directive and the Cyber Solidarity Act, and their related implementation efforts.

3.2 NIS2 Directive[2]

As per *Article 29 - Cybersecurity Information-Sharing Arrangements of the NIS2 Directive*, Member States shall ensure that entities in scope can exchange information among themselves. The Directive does not specify particular requirements, intentionally referring to “arrangements” and allowing Member States to identify the best approach. It does not mandate the sharing of information, leaving it to entities to decide when to do so, on a voluntary basis.

However, the Directive does instruct Member States to provide the necessary support for exchanging information, namely “facilitating the establishment” of such arrangements, exchanging best practices, and providing guidance. This is an important step in the right direction to creating a level playing field in information sharing across all US Member States.

More specifically, Article 29 refers to “dedicated ICT platforms and automation tools, content and conditions” that can be defined by the established arrangements.

Given the discretion left by the official text of the Directive, Member States will need to weigh the costs and benefits of different approaches, ranging from minimalistic to extensive. At a minimum, Member States should actively engage their national audiences to gather needs and challenges that can be addressed within the framework of the NIS2

[2] EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex (europa.eu)

Directive. They should also start gathering information to inform their guidance towards their national audiences. This could involve providing structured information about the various existing information-sharing models, including an overview of collaboration models, rules, platforms adopted, data formats, etc.

While having a clear picture of all alternatives can be helpful, Member States could also work more actively with their national entities to establish or further develop these arrangements together. It is essential to keep into account that mutual trust, buy-in, and collaboration are foundational ingredients in information sharing. No top-down directions can fully sidestep these challenges. Therefore, shaping this process from the outset with a strong involvement of national entities is strongly encouraged.

Another aspect not to be overlook is the variation in maturity levels across the Union. Some Member States will be much further ahead in this journey, with strong skills and competencies at the national level, already sketched out information sharing models. Similarly, these countries may also have mature national entities, with established information sharing processes. These countries should take advantage of the upcoming legislative initiatives to formalise, consolidate, and improve the current state. For other countries, on the other hand, it will be a great opportunity as well as a greater challenge, as they start out from a less mature position. They should take full advantage of the legislative instruments at their disposal to support the establishment and development of a national information sharing ecosystem.

Concretely speaking, although there is no shortage of innovative and well-established projects, initiatives such as IRIS could offer valuable suggestions showcasing what end-to-end integrated models are possible to develop or adopt.

3.3 Cyber Solidarity Act

While the NIS2 Directive covers a broad scope and information sharing was dedicated only a single article, the Cyber Solidarity Act has a much stronger focus on this topic. Information sharing, addressed by the ‘European Cybersecurity Alert System,’ represents one of the three core pillars of the latest EU cybersecurity policy (not officially adopted at the time of this writing). Some of its core objectives are particularly focused on enhancing information sharing within and between EU Member States, as indicated in Article 3(2).

Overall, there is a need to improve the *quantity and quality of data and information* in a structured manner. This involves pooling relevant data and information on cyber threats and incidents from various sources within the Cross-Border Cyber Hubs and sharing analysed or aggregated information through Cross-Border Cyber Hubs, and where relevant, with the CSIRTs Network.

Beyond exploring and developing innovative solutions, research projects and pilots supported by EU funding, such as IRIS, should serve as a proven baseline because they concretely demonstrate the existing challenges and the available solutions, for example in terms of technological, physical, organizational, legal, and logical structures for data collection, data processing, and data distribution and related decisions. Looking forward, these projects should be further structured and expanded across multiple countries with the involvement of additional stakeholders. The experience developed over three years with the IRIS Consortium should not be wasted, and all Consortium members should be actively engaged, capitalizing on the experience they have gained.

Another core objective of the Cyber Solidarity Act's 'European Cybersecurity Alert System' is the production of *actionable* information and cyber threat intelligence. This involves collecting and supporting the production of high-quality, actionable information and cyber threat intelligence through the use of state-of-the-art tools and advanced technologies and sharing that information and intelligence.

One main issue in the information sharing field is not necessarily information access. While more information could be shared, there is a significant amount of information already available. The primary pain points concern the lack of high-quality and actionable information, as properly indicated by the Cyber Solidarity Act. Producing high-quality intelligence is inherently challenging due to the nature of the field, information asymmetry, resource-intensive research and analysis, high-tempo operations, and tools reproducibility and reuse.

Further structuring the entire ecosystem (e.g., with institutionalised and funded structures like the Cross-Border Cyber Hubs) is the first step, yet additional measures are needed, such as leveraging tools and technologies. Specifically, tools and technologies should be used to support analysts in parsing large volumes of information, correlating and comparing different indicators, identifying trends, and sharing them with other entities or response teams.

Automation should be employed to collect data from various sources and merge it in a standardized fashion. This is particularly relevant for fields like IoT and smart cities, where the number of devices, their types, and data formats can be excessively high to maintain a continuous, detailed, yet manual overview. The same principle applies to both inputs and outputs, considering the range of solutions used by IT, cybersecurity, and other functional teams to process all this data.

While several tools and solutions are already available, both open source and commercial, one of the pain points identified is the integration of different tools. This is precisely why the IRIS project provides unique insights, showcasing its integrated architecture, which consists of components traditionally handled by different solutions.

There is an urgent need to support this transition. While more mature teams and entities have developed custom solutions and integrations, the broader ecosystem seriously lack the resources and skills for a similar approach. In addition, even if resources were available, this approach is not scalable in an efficient way. To expand information sharing across the Union, more off-the-shelf, end-to-end, streamlined, and easy-to-use solutions must be available, without expecting entities to invest significant resources in integrations. The IRIS project tested and demonstrated the feasibility of this approach. Both the final architecture and the lessons learned by the Consortium should be highly valued in this regard.

Building the ecosystem and integrating existing solutions are important steps supported by the Cyber Solidarity Act. Another core objective of the 'European Cybersecurity Alert System' has an even more tangible focus: the development of tools and technologies. This includes providing services and activities for the cybersecurity community in the Union, including contributing to the development of advanced tools and technologies, such as artificial intelligence and data analytics tools.

EU research funding should continue to play a key role in this context, especially as new technologies (e.g., AI foundational models), their applications (e.g., AI use cases), or their adoption (e.g., IoT use in cities) come to fruition.

Beyond the technological focus, there are important observations to consider concerning processes and management. Due to the intrinsic nature of complex processes involving multiple stakeholders, these are inherently prone to errors, time-consuming, and resource-intensive, and as a result often leading to delays. Two recommendations are worth highlighting. First, there is a need to crowdsource the development of playbooks for an increasing number of use cases and their widespread adoption. This should be done by the most qualified professionals, researchers, and practitioners with the appropriate skills, experience, and overview. The broader national audience should just be granted access to them. Second, entities should invest resources in customizing playbooks to their own environments rather than developing comprehensive playbooks covering the end-to-end process, from detection to threat intelligence to response, where tailored threat assessments are already available.

Additionally, processes are a key area often underrated. Technological solutions, like automated tools, can play an important role in simplifying and streamlining information sharing, communication, and reporting lines. More attention and related funding in needed in this direction. Policymakers should strongly emphasize this area of work, especially considering the focus on cybersecurity policy implementation anticipated for the coming years.

3.4 Conclusions

In summary, cybersecurity challenges may seem novel, yet they are rooted in longstanding issues. The European Union's recent policies, namely the NIS2 Directive and the Cyber Solidarity Act, strive to enhance the framework for information sharing among cybersecurity stakeholders.

The NIS2 Directive establishes a flexible approach, allowing Member States to tailor information-sharing arrangements to their specific needs. This flexibility, however, requires a proactive stance from Member States to engage with national entities, assess their needs, and develop effective strategies for information exchange. Member States should adopt and adapt these models to improve their national frameworks, building on the lessons learned from established projects like IRIS.

The Cyber Solidarity Act, with its focus on the European Cybersecurity Alert System, underscores the importance of elevating both the quantity and quality of shared data. This policy emphasizes the need for structured data sharing, high-quality actionable intelligence, and the integration of advanced technologies. The IRIS project serves as a valuable case study, demonstrating the effectiveness of integrated architectures and the necessity for scalable, user-friendly solutions. As the ecosystem expands, leveraging existing tools and focusing on end-to-end solutions will be crucial for broadening participation and enhancing overall effectiveness.

Looking ahead, it is essential also for EU research funding to support ongoing advancements in technologies and processes, particularly those that improve automation and integration. Furthermore, the development and adoption of playbooks and automated tools should be prioritized to streamline complex processes and enhance efficiency.

By following these recommendations, EU policymakers can contribute, in a concrete manner, to improving the information sharing challenges the sector has been facing for decades. This is an inherently complex line of work that should not be left behind.

4 References

[1] Article 29 Working Party (2017). Guidelines on Data Protection Impact Assessment. Retrieved on 02.07.2024 from: https://ec.europa.eu/newsroom/article29/items/611236/en.

[2] European Parliamentary Research Service (2020). The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence. Retrieved on 02.07.2024 from: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf;

[3] The Information Commissioner's Office. A guide to the data protection principles. Retrieved on 02.07.2024 from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/.