ENISA
AI CYBERSECURITY CONFERENCE

7 June, Brussels

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

INSPIRING FUTURES

AI Cybersecurity Conference

Brussels 7th June 2023

enisa

THE EU CYBERSECURITY AGENCY

Research and innovation needs and challenges for AI in cybersecurity

AI & Cybersecurity R&I in Europe: Navigating between rhetoric and reality!

Gianluca Misuraca
Founder & Vice President, Inspiring Futures

Outline

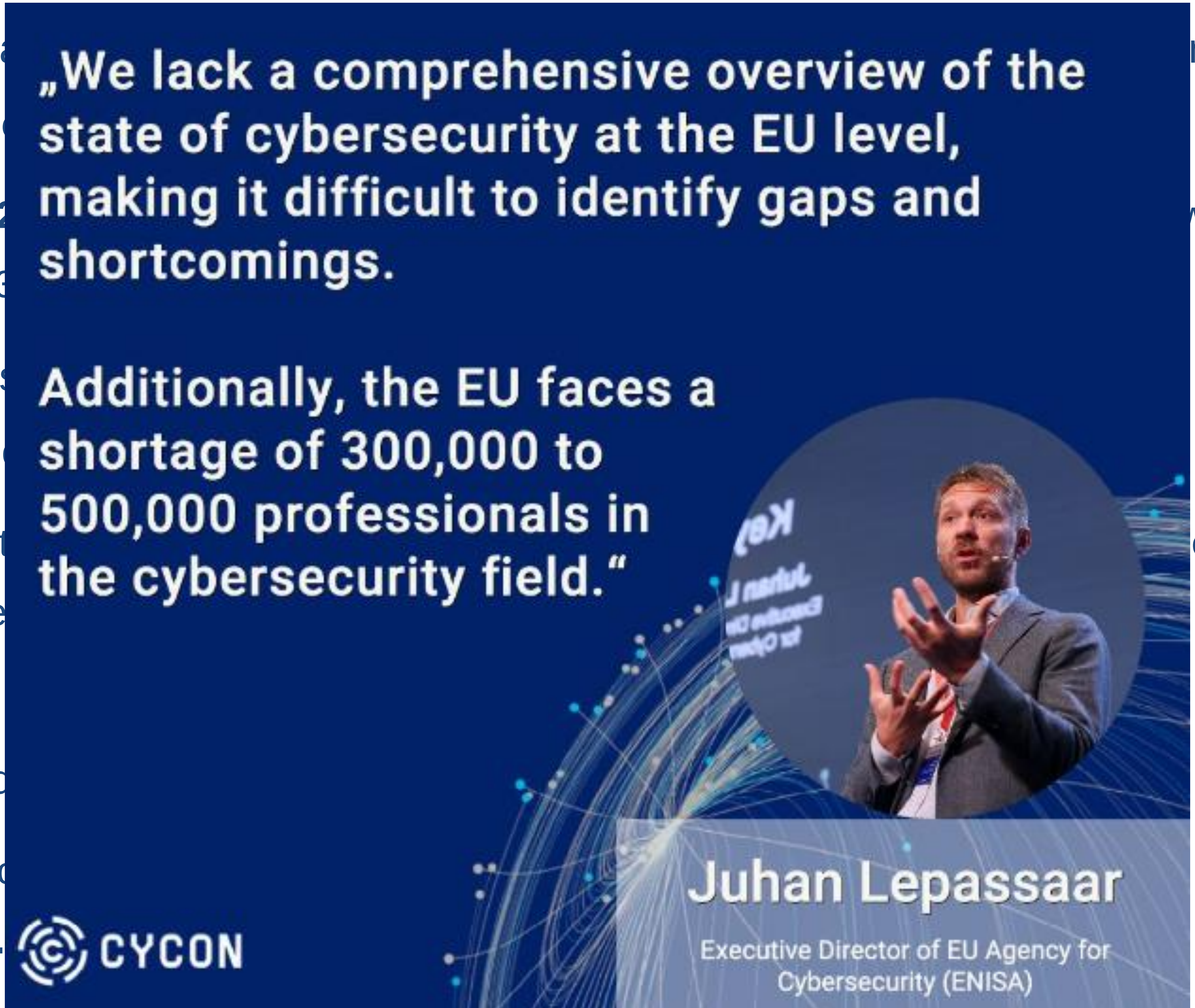
1. Context & Background

2. Results & Insights

3. Gaps & Recommendations

Context: AI & Cybersecurity, are we ready?

- Cyber… nd
  the ris…
  - In 2… wth
    of 3…
- Cybers…
  advan…
  - But… elp
    pre…
- **AI for**
  gained…
  - Acc… **of**
    63.



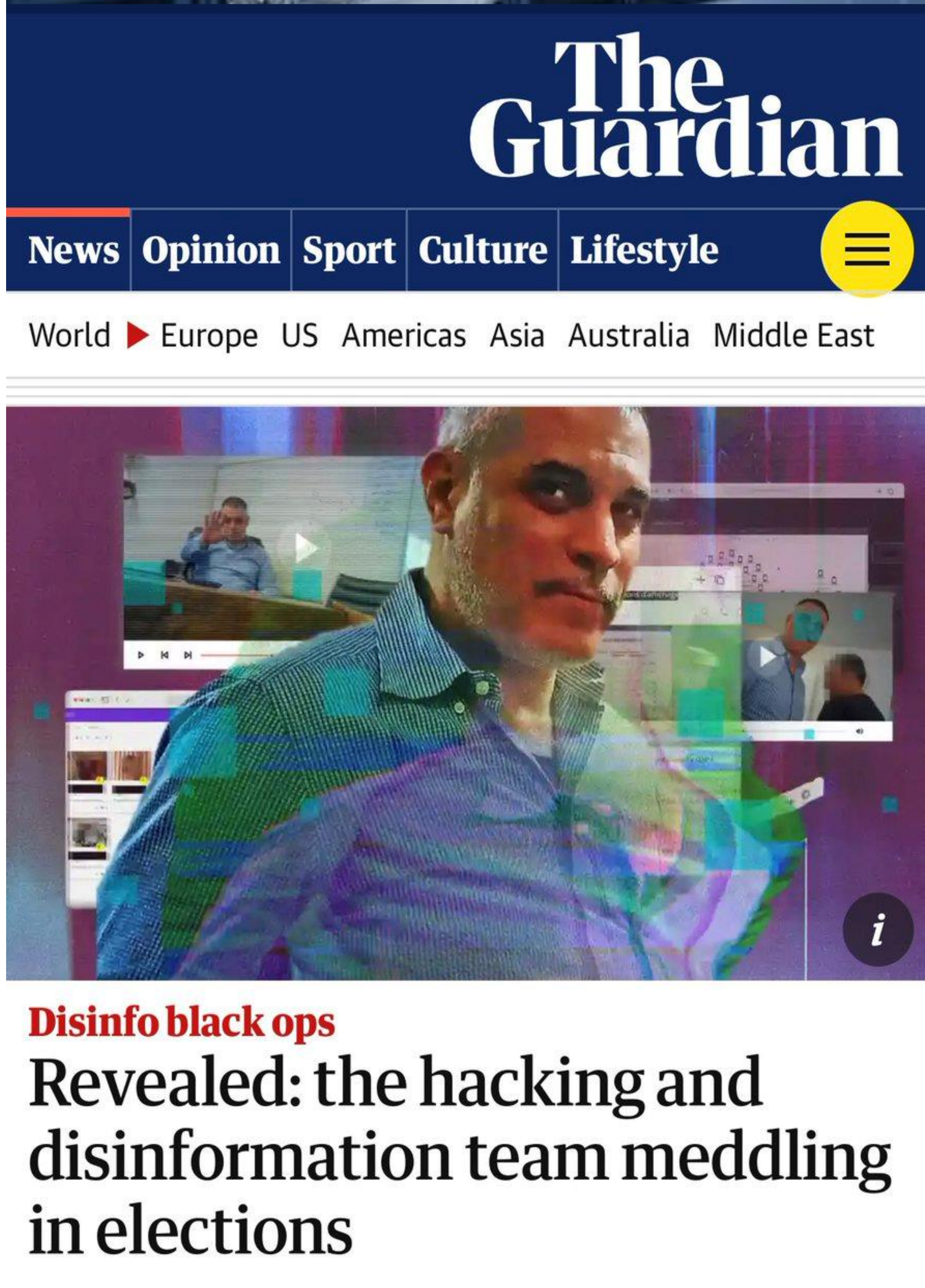
„We lack a comprehensive overview of the state of cybersecurity at the EU level, making it difficult to identify gaps and shortcomings.

Additionally, the EU faces a shortage of 300,000 to 500,000 professionals in the cybersecurity field."

Juhan Lepassaar

Executive Director of EU Agency for Cybersecurity (ENISA)

CYCON



Disinfo black ops

Revealed: the hacking and disinformation team meddling in elections

Background: exploratory studies on AI and Cybersecurity for ENISA (2021 and 2022)

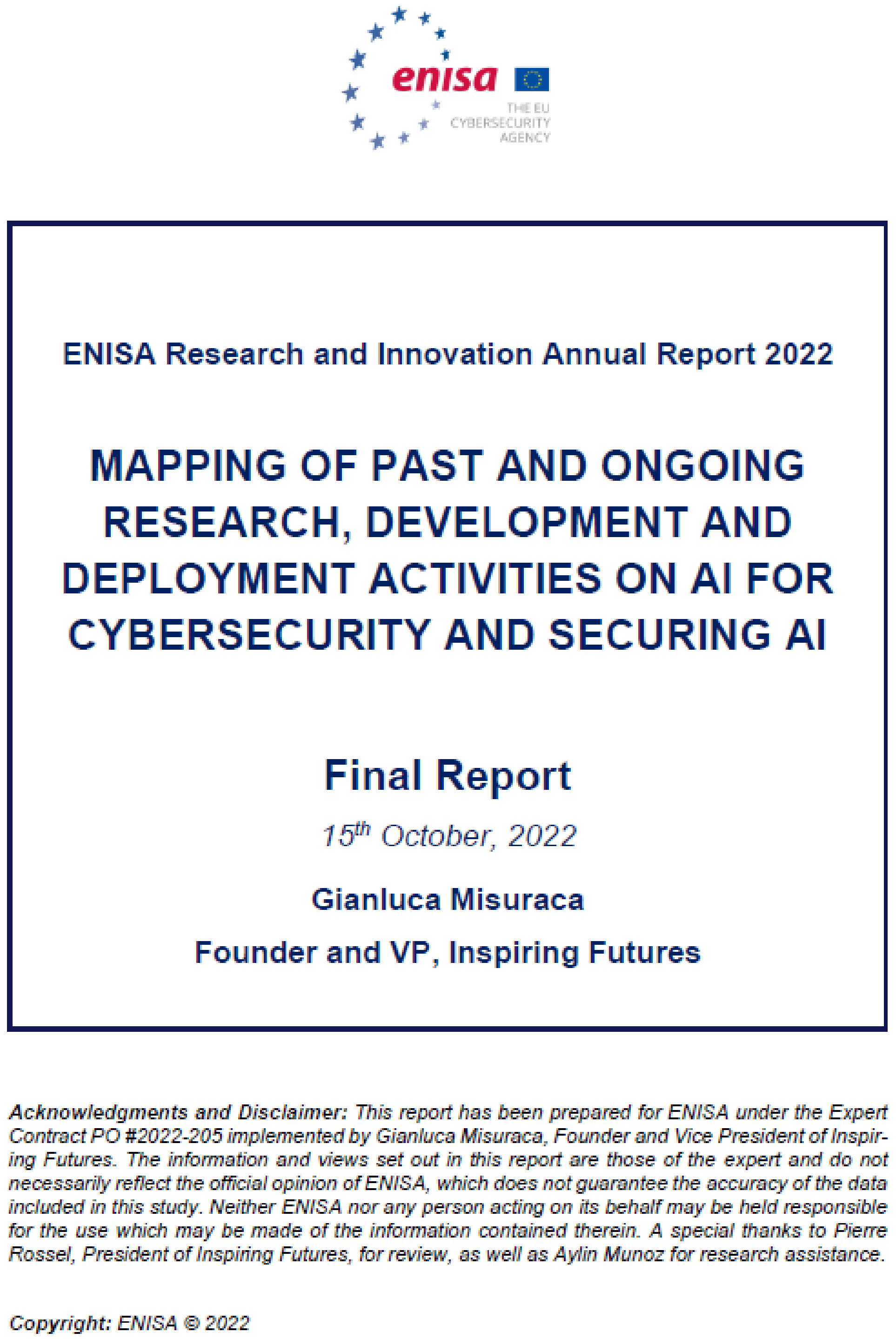
ENISA Research and Innovation Annual Report

Exploring the impact of Artificial Intelligence on cybersecurity issues

Gianluca Misuraca
Co-Founder & Vice President, Inspiring Futures

FINAL
- 24th September 2021 -

***Acknowledgments and Disclaimer:** This report has been prepared for ENISA under the Expert Contract PO #2021-210 with Gianluca Misuraca. The information and views set out in this report are those of the expert and do not necessarily reflect the official opinion of ENISA, which does not guarantee the accuracy of the data included in this study. Neither ENISA nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein. The author is grateful to Pierre Rossel, President of Inspiring Futures for comments and review and Giovanni Zenga for research and editorial support in preparation of the final report.*



ENISA Research and Innovation Annual Report 2022

MAPPING OF PAST AND ONGOING RESEARCH, DEVELOPMENT AND DEPLOYMENT ACTIVITIES ON AI FOR CYBERSECURITY AND SECURING AI

Final Report
15th October, 2022

Gianluca Misuraca
Founder and VP, Inspiring Futures

***Acknowledgments and Disclaimer:** This report has been prepared for ENISA under the Expert Contract PO #2022-205 implemented by Gianluca Misuraca, Founder and Vice President of Inspiring Futures. The information and views set out in this report are those of the expert and do not necessarily reflect the official opinion of ENISA, which does not guarantee the accuracy of the data included in this study. Neither ENISA nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein. A special thanks to Pierre Rossel, President of Inspiring Futures, for review, as well as Aylin Munoz for research assistance.*

ENISA Research and Innovation Annual Report 2022

CYBERSECURITY RESEARCH NEEDS AND PRIORITIES

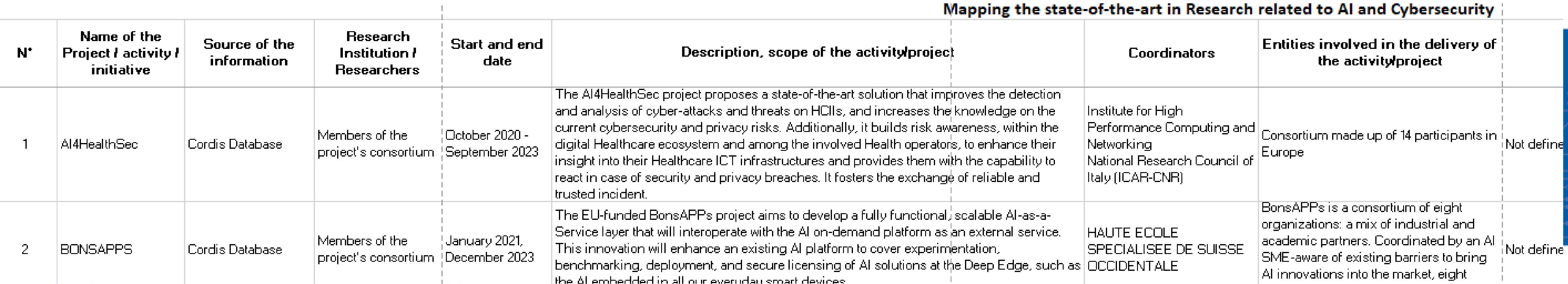
A GAP ANALYSIS AND OPPORTUNITIES FOR FUTURE RESEARCH

Final Report
22nd October, 2022

Francesco Molinari

***Acknowledgments and Disclaimer:** This report has been prepared for ENISA under the Expert Contract PO #2022-206 implemented by Francesco Molinari. The information and views set out in this report are those of the expert and do not necessarily reflect the official opinion of ENISA, which does not guarantee the accuracy of the data included in this study. Neither ENISA nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein. A special thanks to Gianluca Misuraca, Vice President of Inspiring Futures for coordination and supervisory role in the implementation of the study.*

Outcome: ENISA briefs and inventory of projects



Mapping the state-of-the-art in Research related to AI and Cybersecurity

N°	Name of the Project / activity / initiative	Source of the information	Research Institution / Researchers	Start and end date	Description, scope of the activity/project	Coordinators	Entities involved in the delivery of the activity/project	
1	AI4HealthSec	Cordis Database	Members of the project's consortium	October 2020 - September 2023	The AI4HealthSec project proposes a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs, and increases the knowledge on the current cybersecurity and privacy risks. Additionally, it builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with the capability to react in case of security and privacy breaches. It fosters the exchange of reliable and trusted incident.	Institute for High Performance Computing and Networking National Research Council of Italy (ICAR-CNR)	Consortium made up of 14 participants in Europe	Not define
2	BONSAPPS	Cordis Database	Members of the project's consortium	January 2021, December 2023	The EU-funded BonsAPPs project aims to develop a fully functional, scalable AI-as-a-Service layer that will interoperate with the AI on-demand platform as an external service. This innovation will enhance an existing AI platform to cover experimentation, benchmarking, deployment, and secure licensing of AI solutions at the Deep Edge, such as the AI embedded in all our everyday smart devices	HAUTE ECOLE SPECIALISEE DE SUISSE OCCIDENTALE	BonsAPPs is a consortium of eight organizations: a mix of industrial and academic partners. Coordinated by an AI SME-aware of existing barriers to bring AI innovations into the market, eight complementary partners participate: six	Not define
					vernance structures ractice examples of partners.	Professor Dr. Kai Rannenberg	With over 100 cybersecurity projects between them, the CyberSec4Europe consortium members cover a wide spectrum of cybersecurity issues: 14 key cybersecurity domain areas, 11 technology/applications elements and	Public sec SMEs, res software ir organisati regulators
					d unified IIoT pation, detection,	IDRYMA TECHNOLOGIAS KAI EREVNAS (Greece)	Consortium made up of universities and private companies in Europe	Not define
					y challenges IL) techniques and	FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATALUNYA (Spain)	Consortium made up of 18 partners (universities and private companies) in Holland, Germany, Portugal, Spain, UK, Austria, Greece, Cyprus and South Korea	CARAMEI commerci products f automotive
					cus on IOT & neration Cyber-	THE UNIVERSITY OF READING (UK)	The Critical-Chains Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users	Finance s

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

RESEARCH AND INNOVATION BRIEF

Annual Report on Cybersecurity Research and Innovation Needs and Priorities

MAY 2022

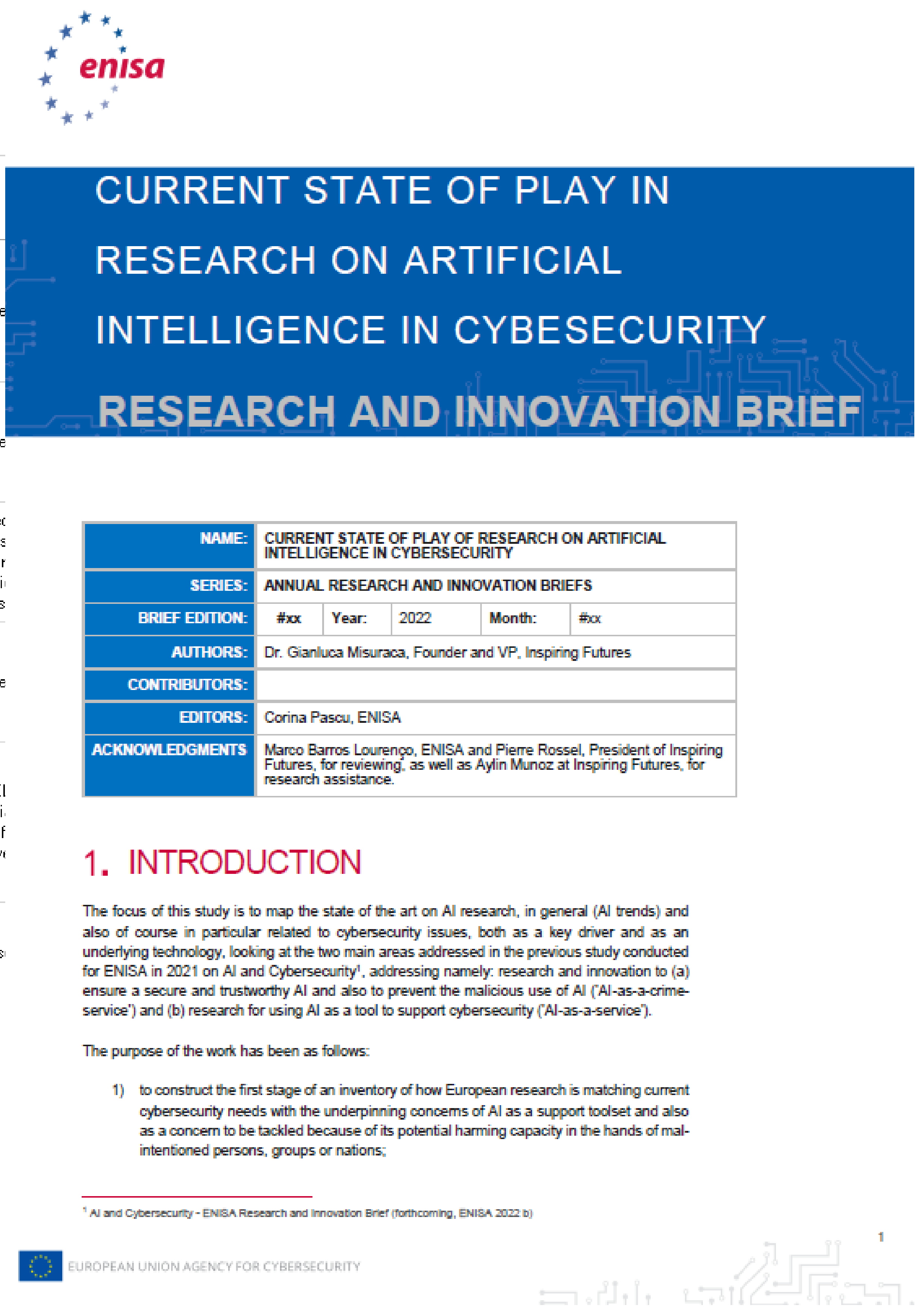
enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

RESEARCH AND INNOVATION BRIEF

Research directions for Artificial Intelligence in Cybersecurity: state-of-the art and futures

JUNE 2022



enisa

CURRENT STATE OF PLAY IN RESEARCH ON ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

RESEARCH AND INNOVATION BRIEF

NAME:	CURRENT STATE OF PLAY OF RESEARCH ON ARTIFICIAL INTELLIGENCE IN CYBERSECURITY				
SERIES:	ANNUAL RESEARCH AND INNOVATION BRIEFS				
BRIEF EDITION:	#xx	Year:	2022	Month:	#xx
AUTHORS:	Dr. Gianluca Misuraca, Founder and VP, Inspiring Futures				
CONTRIBUTORS:					
EDITORS:	Corina Pascu, ENISA				
ACKNOWLEDGMENTS	Marco Barros Lourenço, ENISA and Pierre Rossel, President of Inspiring Futures, for reviewing, as well as Aylin Munoz at Inspiring Futures, for research assistance.				

1. INTRODUCTION

The focus of this study is to map the state of the art on AI research, in general (AI trends) and also of course in particular related to cybersecurity issues, both as a key driver and as an underlying technology, looking at the two main areas addressed in the previous study conducted for ENISA in 2021 on AI and Cybersecurity[1], addressing namely: research and innovation to (a) ensure a secure and trustworthy AI and also to prevent the malicious use of AI ('AI-as-a-crime-service') and (b) research for using AI as a tool to support cybersecurity ('AI-as-a-service').

The purpose of the work has been as follows:

1) to construct the first stage of an inventory of how European research is matching current cybersecurity needs with the underpinning concerns of AI as a support toolset and also as a concern to be tackled because of its potential harming capacity in the hands of mal-intentioned persons, groups or nations;

[1] AI and Cybersecurity - ENISA Research and Innovation Brief (forthcoming, ENISA 2022 b)

Selected **results** from exploratory study (2021)

- **AI is needed** to help identify anomalies, support the learning and optimisation of verification routines, propose useful predictive clues, define and follow up risk profiles, and in general improve user behavior checking and help reacting to threats and intrusion risks;

- **AI also provides critical information for AI-aided attacks**, in a landscape of uncertain mastery in which fake news and disinformation nurture a propitious climate for cybercrime and cyberwar

- **The horizontal vs. the vertical view**: Cybersecurity is hardly limited to the technical fortress whose perimeter it is supposed to defend, but includes also all the transmission links with external partners, using all sorts of connected devices and systems to be watched for

  - A crucial element to consider is how all **employees in any organisation** to be defended are part of the cybersecurity and AI ecosystem: <u>humans in the loop are often the entry point for attacks</u>

  - **IoT** and incoming **5G and 6G Networks systems** may represent the weakest elements of the AI and cybersecurity value chain, a concern also relevant for Cloud and even blockchain-related technologies

Mapping of research on AI and Cybersecurity in the EU (2022)

Support to ENISA R&I to **assess existing and past research, development and deployment projects at the interplay between cybersecurity and AI** through :

- An inspiring review and mapping of the state of the art of EU AI and cybersecurity research through analysis of an initial inventory and gap analysis in the two main areas addressed in the previous study conducted in 2021, namely:

  a) **'AI-as-a-crime-service‘:** research and innovation to ensure a secure and trustworthy AI and to prevent the malicious use of AI; and

  b) **'AI-as-a-service‘:** research for using AI as a tool to support cybersecurity

- In addition, **an exploratory reflection on the implications for cybersecurity of emerging Web3.0 developments,** including the growth of the “dark side” of the Metaverse

Insights from the analysis of the EU landscape on AI and Cybersecurity

1. **Diversity**: from basic research to prototyping and AI-aaS, specialised or generic, with good geographical spread, topical diversity, and deliverable types: prototypes, demos, simulators, reports, courses, workshops, etc.)
2. **Collaborations**: with the presence of small and large consortia, EU-funded and MS projects, mainly from research institutions, but involving also an interesting variety of private players, from big industry to SMEs)
3. **Specialisations:** high variety of focus areas, including critical infrastructures, automated vehicles, IoT security cryptography, healthcare, finance, cyberdefence, terrorism, smart cities, industry 4.0, and public sector
4. **Critical infrastructures and IoT reinforcements:** several EU projects are working on different ways to reinforce IoT cybersecurity, often with the help of AI, in domains such as: industry, health, smart cities and public sector
5. **Trust-oriented explanatory research:** several projects engaged on explainability and shareability, as well as privacy protection, law enforcement and regulatory governance issues,
6. **Ethics/privacy:** in addition to several EU-funded projects which aims to ensure protection of human rights, for instance through data anonymisation, and some projects addressing the concern of ensuring **Human oversight** through situational awareness, explainability and inclusion in decision-making
7. **Innovative-minded concepts using AI tools and solutions**: many projects attempt at making AI more accessible, understandable, verifiyable and easily usable: promoting in practice the adoption of AI–aaS

AI, cybersecurity and the **Web3.0**

- The progressive impact of AI on cybersecurity also represents the expansion and modification of the threat landscape with high chances of AI systems becoming subject to manipulation themselves
  - ➢ Human surveillance and audit are still essential due to the changes in the learning abilities of these systems which make it difficult to assess new behavioural patterns

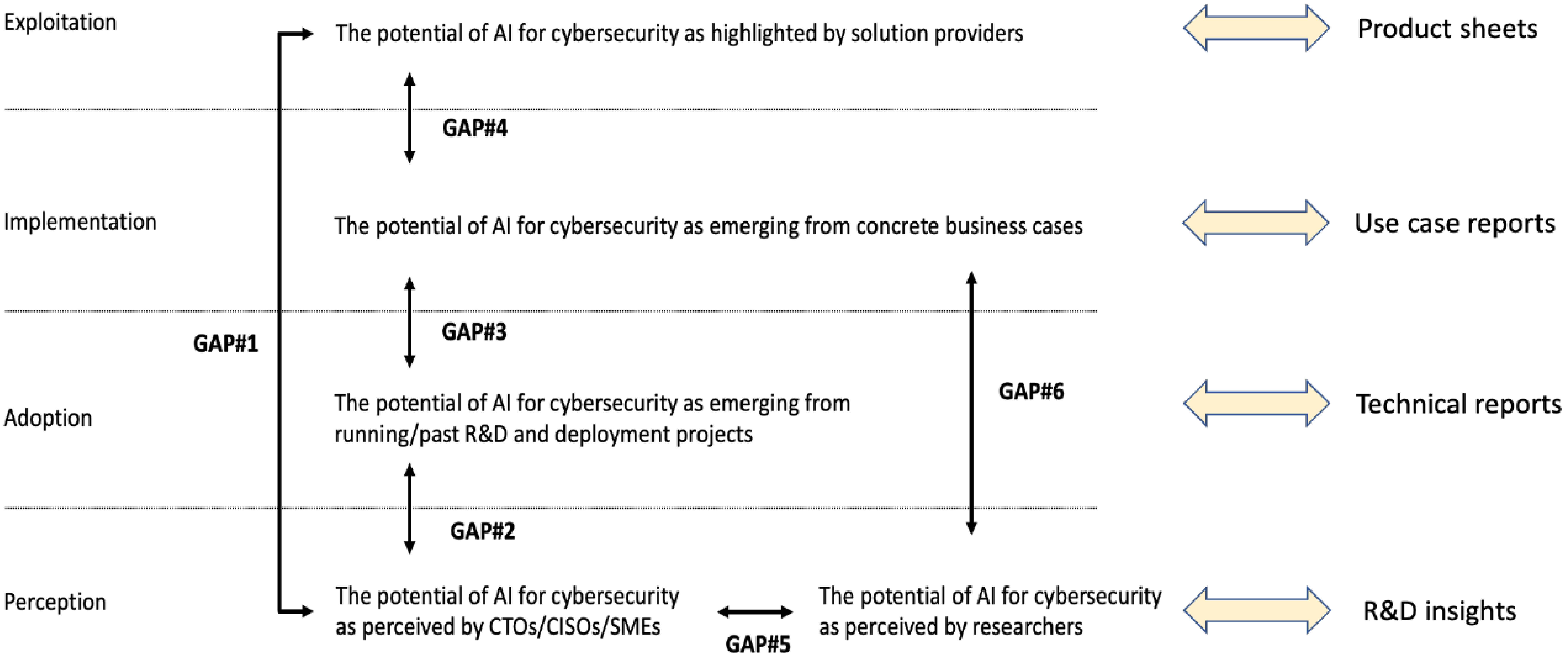
- This scenario poses a riddle urged to be solved as we head into the Web 3.0 era
  - ➢ The Web3.0 is mainly characterized by the decentralized use of data that can only be securely accomplished and managed through combining blockchain-related technologies and AI, with applications introducing all the cybersecurity weaknesses of social computing along the way

- More crucial than ever is the need to examine the cyber risks involved, as well as the actions being taken to prevent security breaches, with a specific regard to he development of generative AI as it is quickly amplifying cybersecurity risks

Emerging -now consolidating- **trends** not to forget!

- The EU ambition to re-affirm digital sovereignty
  - and the related cybersecurity conditions underpinning it
- The porous continuum between fake news and disinformation, cybercrime, cyber and hybrid wars (as the persisting conflict in Ukraine confirmed)
  - the importance of Advanced persistent threats (APTs), especially in the ambiguous relations with non-democratic countries and hackers' manoeuvrings (e.g. Pegasus spyware, but also the Nord Stream and other war-related mysteries…)
- Critical infrastructures as key stake in the context of hybrid wars and attacks
  - growing acknowledgment of the need for incidents' follow-up, as done in aviation
- Need to continuously monitor and evaluate the potential linked with some of the predictions presented as trends and anticipate trends through simulation!

Gap analysis



Exploitation

The potential of AI for cybersecurity as highlighted by solution providers

Product sheets

GAP#4

Implementation

The potential of AI for cybersecurity as emerging from concrete business cases

Use case reports

GAP#3

GAP#1

GAP#6

Adoption

The potential of AI for cybersecurity as emerging from running/past R&D and deployment projects

Technical reports

GAP#2

Perception

The potential of AI for cybersecurity as perceived by CTOs/CISOs/SMEs

GAP#5

The potential of AI for cybersecurity as perceived by researchers

R&D insights

Source: Molinari for ENISA, 2022

Results from the **gap analysis**

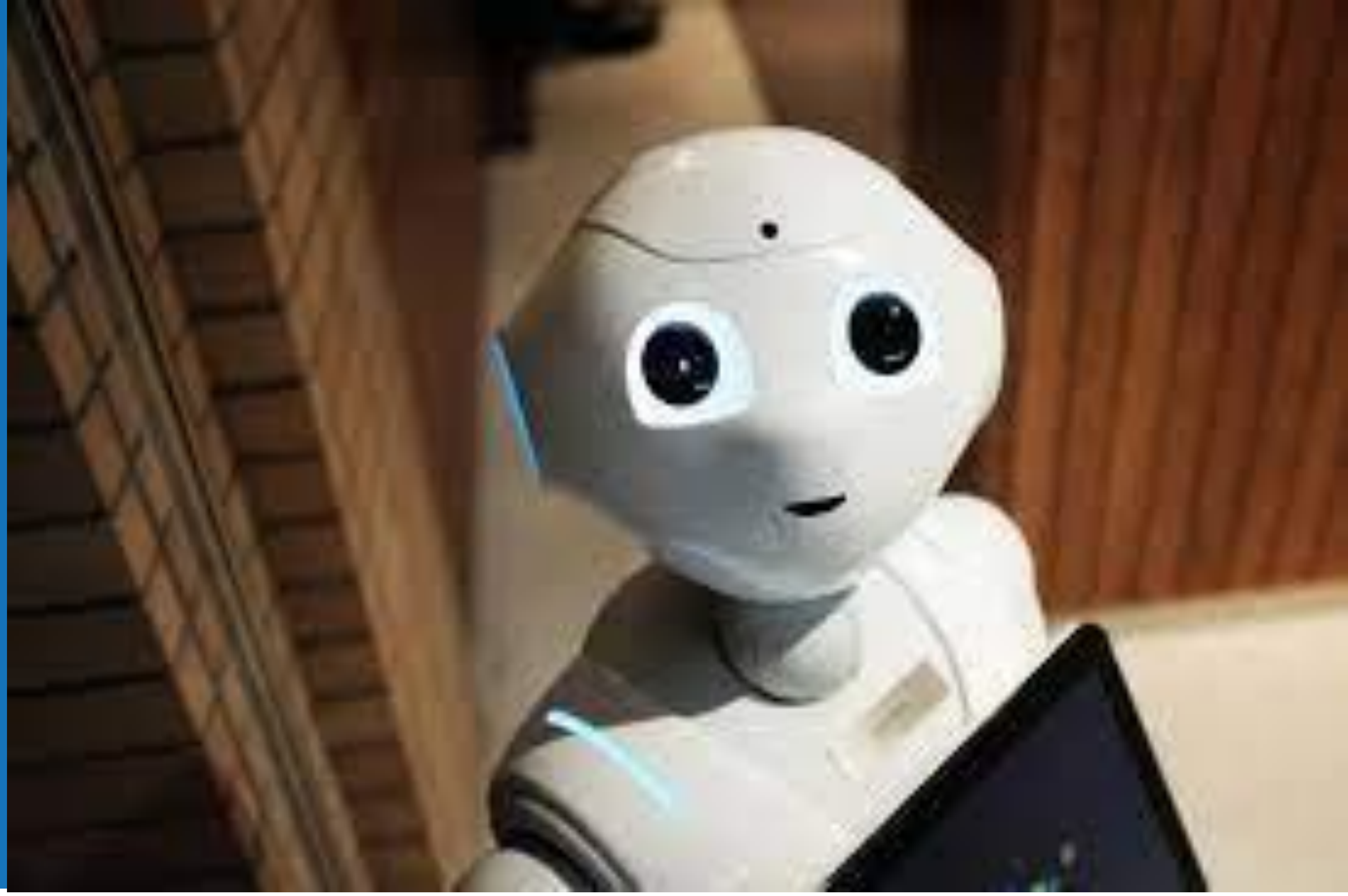
1. **Lack of adequate information and knowledge** regarding the potential of AI solutions for Cybersecurity, or because of the experimental nature of most AI solutions;
2. **R&D and deployment projects are not sufficiently well documented** to ensure that the organisations that could potentially adopt them perceive the potential in full;
3. **Too few demonstration activities that can provide concrete/convincing business cases** for the value and potential of AI solutions for Cybersecurity and be replicated;
4. **Only a minority of the prototypes/demonstrators refined in the context of R&D and innovation activities enters actually the market/**have sound business cases;
5. **A perception gap between the researcher and the business community** which hinders the efforts to match the design of R&D projects with market solutions;
6. **Limited capacity of R&I projects to solve existing or potentially emerging problems associated** with business-driven application domains

INSPIRING FUTURES

Recommendations

1. Extend the emergent phenomenon of **“AI as a service”** and made complementary to **“Cybersecurity as a service”**, to enhance the strength of association between the two;
2. Promote **AI interpretability and explainability** through appropriate initiatives (e.g. funded deployment actions, introduction of standards and certification models)
3. Further **experimentation and cross-sectorial transfer of R&D results**, including “ad hoc” measures to track and support engineering of available results and business cases (e.g. dedicated spaces in the EIC work programme to AI for Cybersecurity);
4. Funding calls should **prioritise projects “with a purpose”** and repositories of successful cases be created, to **promote replicability/transfer** across industrial sectors;
5. Prioritise solutions demonstrating the best fit into an ideal definition of “scalable” and “multisectoral” and **incentivize the of use of Sandboxes to finalise productization**;
6. Invest in **capacity building, raising awareness activities and multi-disciplinary collaboration**, and accompany prototype testing activities with implementation guidelines

Watch out what’s next…



INSPIRING FUTURES

….and get Inspired!

gm@inspiringfutures.ch