EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FORESIGHT CYBERSECURITY THREATS FOR 2030 – UPDATE

Executive Summary

MARCH 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use foresight@enisa.europa.eu'
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Rossella Mattioli, Apostolos Malatras, - ENISA, 4CF, PWC

ACKNOWLEDGEMENTS

ENISA's Ad-Hoc Working Group on Foresight on Emerging and Future Cybersecurity Challenges, ENISA Advisory Group, ENISA National Liaison Officers Network and experts from the CSIRTs Network and EU CyCLONe who participated in the workshops and provided feedback.

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. INTRODUCTION

The “ENISA Foresight Cybersecurity Threats for 2030” study represents a comprehensive analysis and assessment of emerging cybersecurity threats projected for the year 2030. This collaborative endeavour, spearheaded by European Union Agency for Cybersecurity (ENISA), has employed a structured and multidimensional methodology to assess, forecast, and prioritise potential threats. It was firstly published in 2022, and the current report is its second iteration which reassesses the previously identified top ten threats and respective trends whilst exploring the developments over the course of a year. The assessment yields key findings that shed light on the evolving nature of the cybersecurity landscape:

Dynamic Threat Landscape:

- The analysis underscores the rapid evolution of the threat landscape, marked by dynamic attack vectors. Threat actors, including advanced persistent threats, nation-state actors, and sophisticated cybercriminal organizations, continue to adapt and refine their tactics.

Technology-Driven Challenges:

- The adoption of emerging technologies introduces both opportunities and vulnerabilities. This dual nature of technological advancements necessitates proactive cybersecurity measures to address potential risks associated with their adoption.

Impact of Emerging Technologies:

- Quantum computing and artificial intelligence (AI) emerge as key factors impacting the threat landscape. While these technologies offer significant opportunities, they also introduce vulnerabilities that malicious actors may exploit. The report emphasizes the importance of understanding and mitigating these risks.

Increased Complexity:

- The assessment reveals that the threat landscape is becoming more complex, requiring a sophisticated understanding of evolving tactics and strategies employed by threat actors. This complexity underscores the need for advanced cybersecurity measures.

Proactive Cybersecurity Measures:

- Organizations and policymakers are encouraged to adopt proactive cybersecurity measures to fortify their cybersecurity posture. Understanding the evolving threat landscape and being prepared to address emerging challenges is crucial for building resilience in the digital environment.

Forward-Looking Perspective:

- The review of the "ENISA Foresight Cybersecurity Threats for 2030" is grounded in a rigorous methodology and expert collaboration. The forward-looking perspective provided in the report offers valuable insights and recommendations for stakeholders to prepare for and counter emerging threats.

Resilient Digital Environment:

- By embracing the insights and recommendations from the report, organizations and policymakers can enhance their cybersecurity strategies. This proactive approach aims to ensure a resilient digital environment not only in the year 2030 but also in the evolving landscape beyond.

The “ENISA Foresight Cybersecurity Threats for 2030” study represents a comprehensive analysis and assessment of emerging cybersecurity threats projected for the year 2030.

2. OBJECTIVES

The exercise serves as a strategic initiative to assess, validate, and enhance the ENISA Foresight Cybersecurity Threats for 2030. By leveraging input from experts and stakeholders, the exercise supports evidence-based decision-making, strengthens ENISA's strategic objectives, and contributes to ongoing efforts to address emerging cybersecurity challenges.

The exercise has encompassed two steps: (1) a Delphi survey focusing on threats from the report (Chapter 3), and (2) a workshop focusing on the trends as well as scenarios, both of which were organised in October 2023. The workshop aimed to provide a structured and critical assessment of the ENISA Foresight Cybersecurity Threats for 2030, ensuring its relevance and accuracy in the face of evolving cybersecurity challenges.

The exercise aligns with ENISA's sixth strategic objective. By reviewing and assessing the foresight report, it contributes to a deeper understanding of cybersecurity threats, serving as a basis for awareness activities, and ensuring that stakeholders have a sense of ownership in the cybersecurity initiatives driven by ENISA. This comprehensive approach reflects a commitment to strengthening cybersecurity practices and resilience in the evolving digital landscape.

The target audience of the exercise were stakeholders from the cybersecurity domain including national cybersecurity authorities, national and EU decision makers, experts, and practitioners forming Ad-Hoc Working Group on Foresight on Emerging and Future Cybersecurity Challenges.

3. METHODOLOGY

The methodology employed for the review of the ENISA Foresight Cybersecurity Threats for 2030 involved a combination of the Real-Time Delphi survey technique and a thematic workshop to ensure a thorough and validated review process.

The Delphi technique, a structured and iterative method, was used to gather collective forecasts and expert opinions on likely or possible developments in cybersecurity. 33 experts were invited, and 24 participated in the survey that involved multiple rounds of questionnaires, feedback, and refinement to converge opinions or identify potential developments.

The online workshop, held on October 12, 2023, gathered 10 experts and practitioners. It consisted of two parts: a session reviewing 2030 trends (Chapter 4) and a review of scenarios based on the outcomes of previous steps.

To ensure a quality review, a validation process of the report was conducted, involving the expertise of the Ad hoc Working Group on Foresight for Emerging and Future Cybersecurity Challenges, consultation with the ENISA National Liaison Officers network, and input from the Advisory Group composed of experts from industry, academia, business, and consumer groups.

The methodology employed for the review of the ENISA Foresight Cybersecurity Threats for 2030 involved a combination of the Real-Time Delphi survey technique and a thematic workshop to ensure a thorough and validated review process.

4. THREATS

The real-time Delphi survey, conducted online with the participation of 24 experts, led to the revision of the top ten cybersecurity threats. The experts contributed assessments regarding the impact and likelihood of various threats, providing a comprehensive view of the cybersecurity landscape. The revised top ten list was formulated based on the multiplication of impact and likelihood scores assigned by the participating experts:

1. **Supply Chain Compromise of Software Dependencies**
2. **Skill Shortage**
3. **Human Error and Exploited Legacy Systems Within Cyber-Physical Ecosystems**
4. **Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [New in Top Ten]**
5. **Rise of Digital Surveillance Authoritarianism / Loss of Privacy**
6. **Cross-border ICT Service Providers as a Single Point of Failure**
7. **Advanced Disinformation / Influence Operations (IO) Campaigns**
8. **Rise of Advanced Hybrid Threats**
9. **Abuse of AI**
10. **Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [New in Top Ten]**

Table 1: New prioritisation of threats

	THREAT	IMPACT * LIKELIHOOD	IMPACT	LIKELIHOOD
1.	**Supply Chain Compromise of Software Dependencies**	17,71	4,21	4,21
2.	**Skill Shortage**	17,20	4,10	4,20
3.	**Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems**	16,69	3,96	4,22
4.	**Exploitation of Unpatched and Out-of-date Systems within the Overwhelmed Cross-sector Tech Ecosystem [Optional]**	16,21	4,05	4,00
5.	**Rise of Digital Surveillance Authoritarianism / Loss of Privacy**	15,34	3,96	3,88
6.	**Cross-border ICT Service Providers as Single Point of Failure**	15,12	4,14	3,65
7.	**Advanced Disinformation / Influence Operations (IO) Campaigns**	14,38	3,42	4,21
8.	**Rise of Advanced Hybrid Threats**	14,03	3,68	3,81
9.	**Abuse of AI**	13,22	3,43	3,86

10.	**Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure [Optional]**	12,99	3,68	3,53
11.	**Lack of Analysis and Control of Space-based Infrastructure and Objects**	12,52	3,63	3,45
12.	**Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data**	12,29	3,39	3,63
13.	**Increased Digital Currency-enabled Cybercrime [Optional]**	10,25	3,06	3,35
14.	**Manipulation of Systems Necessary for Emergency Response [Optional]**	10,02	3,27	3,07
15.	**Tampering with Deepfake Verification Software Supply Chain [Optional]**	9,83	3,00	3,28
16.	**AI Disrupting/Enhancing Cyber Attacks [Optional]**	9,78	3,07	3,19
17.	**Malware Insertion to Disrupt Food Production Supply Chain [Optional]**	9,33	3,11	3,00
18.	**Exploitation of E-health (and Genetic) Data [Optional]**	9,32	3,11	3,00
19.	**Attacks Using Quantum Computing [Optional]**	7,32	2,76	2,65
20.	**Disruptions in Public Blockchains [Optional]**	5,96	2,47	2,41
21.	**Technological Incompatibility of Blockchain Technologies [Optional]**	5,91	2,25	2,63

Key takeaways from the review of cybersecurity threats, based on the Delphi survey, highlight the dynamic nature of the threat landscape, and shifts in experts' perceptions between 2022 and 2023:

Continued Significance of Threats:

- Threats such as "Supply Chain Compromise of Software Dependencies" and "Advanced Disinformation/Influence Operations (IO) Campaigns" remain significant, despite experiencing slight declines in perceived prominence. These threats continue to pose substantial risks to cybersecurity.

Shifts in Perceived Impact and Likelihood:

- "Rise Of Digital Surveillance Authoritarianism/Loss of Privacy" shows a slight decline in both impact and likelihood, indicating a nuanced perspective on the long-term implications of digital surveillance practices.

Intensification of Long-Term Threat Perspectives:

- Threats like "Skill Shortage" and "Cross-border ICT Service Providers as a Single Point of Failure" have somewhat intensified in experts' perception. This suggests a growing recognition of the long-term challenges posed by these factors.

AI-Related Threats Gain Likelihood:

- "Abuse of AI" and "AI Disrupting/Enhancing Cyber Attacks" have gained likelihood. This aligns with the increasing coverage of AI applications at scale and the ethical considerations surrounding AI use. Concerns about public over-reliance on AI and the potential blind spots introduced by probabilistic threat detection methods are highlighted.

Exclusions from Top 10:

- "Lack of Analysis and Control of Space-based Infrastructure and Objects" and "Targeted Attacks Enhanced by Smart Device Data" were excluded from the top 10 threats. This suggests a reassessment of their immediate impact compared to other emerging threats.

New Entrants in Top 10:

- "Exploitation of Unpatched and Out-of-date Systems Within the Overwhelmed Cross-sector Tech Ecosystem" and "Physical Impact of Natural/Environmental Disruptions on Critical Digital Infrastructure" moved up from lower positions to be included in the revised top 10. This reflects a heightened awareness of the vulnerabilities associated with outdated systems and the potential physical impact of environmental disruptions on digital infrastructure.

Table 2: Evolution of threat assessments

	THREAT	IMPACT 2022	LIKELIHOOD 2022	IMPACT 2023	LIKELIHOOD 2023	CHANGE IMPACT	CHANGE LIKELIHOOD	IMP*LIKELIHOOD
1.	**Supply Chain Compromise of Software Dependencies**	5	5	4,21	4,21	**-0,79**	**-0,79**	17,71▼
2.	**Skill Shortages**	4	4	4,10	4,20	**0,20**	**0,20**	**17,20▲**
3.	**Human Error and Exploited Legacy Systems within Cyber-Physical Ecosystems**	4	5	3,96	4,22	**-0,78**	**-0,78**	**16,69▼**
4.	**Rise of Digital Surveillance Authoritarianism / Loss of Privacy**	4	5	3,96	3,88	**-1,13**	**-1,13**	**15,34▼**
5.	**Cross-border ICT Service Providers as a Single Point of Failure**	5	3	4,14	3,65	**0,65**	**0,65**	**15,12▲**
6.	**Advanced Disinformation / Influence Operations (IO) Campaigns**	4	5	3,42	4,21	**-0,79**	**-0,79**	**14,38▼**
7.	**Rise of Advanced Hybrid Threats**	4	4	3,68	3,81	**-0,19**	**-0,19**	**14,03▼**
8.	**Abuse of AI**	4	3	3,43	3,86	**0,86**	**0,86**	**13,22▲**
9.	**Lack of Analysis and Control of Space-based Infrastructure and Objects**	4	4	3,63	3,45	**-0,55**	**-0,55**	**12,52▼**
10.	**Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data**	4	4	3,39	3,63	**-0,38**	**-0,38**	**12,29▼**

5. TRENDS

The workshop focused on nine trends susceptible to change by 2030, with participants discussing the potential alterations and impact on cybersecurity:

- **Political trends:**
  - Increased political power of non-state actors; and
  - The increasing relevance of (cyber) security in elections.
- **Economic trends:**
  - Collecting and analysing data to assess user behaviour is increasing, especially in the private sector; and
  - Increasing reliance on outsourced IT Services.
- **Social trends:**
  - Decision-making is increasingly based on automated analysis of data.
- **Technological trends:**
  - The number of satellites in space is increasing and thus our dependency on satellites; and
  - Vehicles are becoming increasingly connected to each other and to the outside world and less reliant on human operation.
- **Environmental trends:**
  - The increasing energy consumption of digital infrastructure.
- **Legal trends:**
  - The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult.

The trend of the increased political power of non-state actors is characterised by the anticipation that global interconnectedness will accelerate.

Participants used the 4CF Stranger Futures workshop method to discuss these trends. All trends, except one (Decision-making based on automated analysis of data), were rated as speeding up beyond their originally presented dynamics in the ENISA 2030 Threats Foresight Report. There was ambiguity about the speed of evolution in the social trend, and experts couldn't reach a consensus on whether it is moving faster or slower.

Experts expressed concerns about how these trends might impact cybersecurity, and some anticipated the need for specific EU regulations to address their negative influences. The evolving nature of these trends adds complexity to the cybersecurity landscape, requiring proactive measures to address emerging challenges.

The trend of the **increased political power of non-state actors** is characterised by the anticipation that global interconnectedness will accelerate, fostering interactions among non-state actors at a pace that may surpass the regulatory capacity of nation-states. This acceleration is expected to result in a diminishing influence of traditional nation-states, particularly in their ability to control and regulate these evolving forms of interactions. While the trend points towards an increase in the political power of non-state actors, there are nuanced perspectives. Positive elements include state initiatives to assert control, and cyber diplomacy is seen as a mitigating force against potential adverse consequences. The evolving landscape emphasizes the need for diplomatic and regulatory strategies to address the challenges posed by increased non-state actor influence.

The trend of **collecting and analysing data to assess user behaviour** is experiencing a significant increase, particularly in the private sector. This trend involves leveraging data for automated decision-making processes, primarily focused on improving customer targeting and reducing operational costs. The increasing digitalization of various aspects of life and advancements in AI algorithms contribute to the growth of this trend. While this trend presents significant opportunities, experts highlight the importance of addressing inherent challenges.

These include the need for accurate and context-aware analysis, addressing biases in behavioural profiling, acknowledging the potential limitations of data-driven models, and considering the adaptability of individuals in shaping the outcomes of behavioural analysis.

While the trend of **decision-making relying on automated data analysis** holds significant potential, experts emphasize the need to address associated pitfalls. These include concerns about data quality, the changing dynamics of decision-making, the balance between quantifiable metrics and optimal decisions, and the potential lack of accountability in the face of suboptimal outcomes.

While the **increasing number of satellites** opens up new possibilities for technology and exploration, it also brings about challenges concerns. These include the need for regulatory frameworks, addressing space traffic and ecological impacts, coordinating satellite operations, and enhancing cybersecurity measures to safeguard satellite infrastructure.

The trend of **controlling personal data** reflects a multifaceted landscape influenced by various factors such as technological advancements, societal priorities, regulatory frameworks, and individual awareness. Addressing the challenges and complexities regarding data control requires a nuanced approach that considers the evolving nature of the digital ecosystem.

The trend of **increasing energy consumption in digital infrastructure** reflects a balance between technological advancements, efforts towards energy efficiency, regulatory landscapes, and uncertainties about future breakthroughs. The dynamic nature of this trend necessitates ongoing monitoring and adaptability to address emerging challenges and opportunities.

6. SCENARIOS

The experts involved in the scenario analysis of the ENISA Foresight Cybersecurity Threats for 2030 have articulated the need for a more nuanced exploration of technological advancements. Their concerns revolve around key thematic areas, emphasizing the importance of addressing trust, privacy, technology misuse, and environmental impacts. They call for specific scenarios addressing water and raw-materials scarcity leading to the collapse of hardware value chains, ethical dilemmas in data-driven decision-making, decentralisation in energy generation, and the role of space technologies in dependencies and vulnerabilities.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu