EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FORESIGHT CYBERSECURITY THREATS FOR 2030 - UPDATE

Extended Report

MARCH 2024

DOCUMENT HISTORY

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

ISBN: 978-92-9204-671-2, DOI 10.2824/349493

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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.

Our aim was to reassess the results of the Foresight Cybersecurity Threats for 2030, identify potential new trends/threats and understand how the previous trends developed over the course of the year. One of the key findings of our assessment was that the threat landscape is rapidly evolving. Specifically, the analysis reveals a dynamic threat landscape marked by evolving attack vectors, including advanced persistent threats, nation-state actors, and intricate cybercriminal organisations. Secondly, there is an increase of technology driven challenges whereby the adoption of emerging technologies introduces both opportunities and vulnerabilities. As a result, this finding is necessitating proactive cybersecurity measures to address potential risks. Tying into this, exercises showed that some of the main emerging technologies impacting the threat landscape include quantum computing and artificial intelligence. While both could result with significant opportunities and challenges, workgroups partaking in this project agreed that these could produce vulnerabilities that malicious actors may exploit.

The review of the “ENISA Foresight Cybersecurity Threats for 2030” grounded in a rigorous methodology and expert collaboration, offers a forward-looking perspective on the evolving cybersecurity landscape. By embracing the insights and recommendations presented in this report, organisations and policymakers can proactively address emerging threats and fortify their cybersecurity posture, ensuring a resilient digital environment in the year 2030 and beyond.

Key takeaways from review of threats

In the realm of cybersecurity threats, a dynamic landscape is revealed through a Delphi survey, showcasing shifts in both perceived impacts and likelihoods of threats between 2022 and 2023.

While some threats like "**Supply Chain Compromise of Software Dependencies" and "Advanced Disinformation/Influence Operations (IO) Campaigns**" have seen slight declines in perceived prominence until 2030, they still pose significant risks. "**Rise Of Digital Surveillance Authoritarianism/Loss of Privacy**" shows a slight decline in impact and likelihood. On the other hand, long term perspectives of threats like "**Skill Shortage**" and "**Cross-border ICT Service Providers as a Single Point of Failure**" have somewhat intensified in experts' perception. "**Abuse of AI**" and "**AI Disrupting/Enhancing Cyber Attacks"** have gained likelihood, which is not surprising given the wide coverage of emergent AI applications at scale and the considerations for ethical use of the newly released, as well as emergent AI models. Additionally, experts have raised concerns, such as the potential blind spots introduced by probabilistic threat detection methods, the public's over-reliance on AI, and the need for strategic reframing in threat assessment. As a result of the exercise two trends were excluded from the top 10 list:

- **Lack of Analysis and Control of Space-based Infrastructure and Objects, and**
- **Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data.**

Two trends moved up from lower positions to be included in the 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.**

Key takeaways from review of trends

In the context of trends, several new or rising dynamics were discussed:

- In political trends, the spotlight is on the increasing power of non-state actors and the growing relevance of cybersecurity in elections and the role of disinformation with AI content.
- In economic trends, the experts point to a dynamic rise in data collection and analysis, but concerns exist regarding the limitations of behavioural profiling and potential decreases in data-driven models.
- In social trends the experts were pointing to the possible turning points in the reliance of decision-making being increasingly on automated data analysis, raising questions about data quality, safety, and accountability.
- In their discussion of economic trends, the experts indicated an ever-increasing reliance on outsourced IT services, creating supply chain complexities and cybersecurity challenges, especially for SMEs.
- In the realm of technology trends, the experts emphasised the faster than previously anticipated growing dependence on satellites and vehicles becoming more connected, with associated cybersecurity and privacy considerations.
- As far as legal trends are concerned, the experts highlight the challenges of controlling personal data in an evolving digital landscape.
- Finally, looking at environmental trends, experts underline the rising energy consumption of digital infrastructure, reminding that this is a strong assumption that may be derailed as soon as 2030 with major advances in energy efficiency or generation.

Scenarios' analysis results

Looking at the scenario analysis in ENISA Foresight Cybersecurity Threats for 2030, experts have the need for more nuanced exploration of technological advancements, with concerns centred around 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.

1. INTRODUCTION

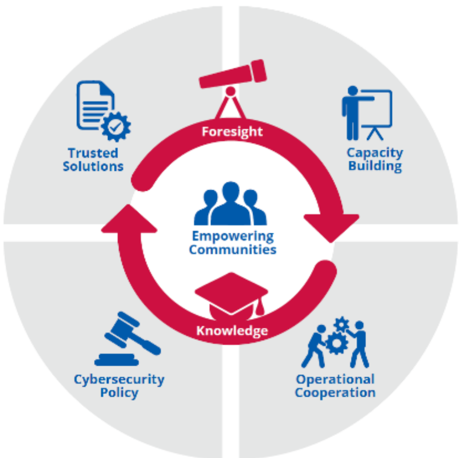
1.1 BACKGROUND

ENISA's strategy proposes concrete goals in the form of seven strategic objectives that will set the priorities for ENISA in the coming years. The strategic objectives[1] are as follows:

1. Empowered and engaged communities across the cybersecurity ecosystem.
2. Cybersecurity as an integral part of EU policies.
3. Effective cooperation amongst operational actors within the Union in case of massive cyber incidents.
4. Cutting-edge competencies and capabilities in cybersecurity across the Union
5. High level of trust in secure digital solutions.
6. Foresight on emerging and future cybersecurity challenges.
7. Efficient and effective cybersecurity information and knowledge management for Europe.

In line with ENISA's sixth strategic objective, "Foresight on Emerging and Future Cybersecurity Challenges[2]", the Agency seeks to improve the EU's cybersecurity resilience, by increasing awareness of future threats and countermeasures amongst its member states and stakeholders. Fulfilling this objective likewise supports the other 6 strategic objectives as it provides input on future threats and challenges.

Figure 1: ENISA Strategic Objectives



To achieve this goal, ENISA has applied its methodological framework grounded in foresight research and future studies that was developed in 2021.[3] The framework, created in collaboration with an interdisciplinary expert group which included futurists, sociologists, business leaders, cybersecurity experts, and others, reviewed the threats and challenges likely to emerge by 2030[4] identified in 2022.

[1] (ENISA, A trusted and Cyber Secure Europe, 2020)
[2] (ENISA, A trusted and Cyber Secure Europe, 2020)
[3] (ENISA, Foresight Challenges, 2021). The framework can be found on page 33 of the report.
[4] (ENISA, Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges, 2021)

1.2 PURPOSE OF THIS EXERCISE

This report summarises the outcomes of the review of ENISA Foresight Cybersecurity Threats for 2030 performed under Cybersecurity Foresight Consultancy Framework Contract.

This 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 purpose of this exercise is to support ENISA's sixth strategic objective. The outcomes have allowed for an informed and evidence-based decision-making on future cybersecurity research. Furthermore, it has formed a basis for further exchange and raising awareness activities run by ENISA, at the same time? Guaranteeing stakeholders' ownership.

1.3 TARGET AUDIENCE

Our main target demographic for this 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.

The purpose of this ad hoc working group is to advise ENISA in developing foresight on emerging cybersecurity challenges and other tasks related to future cybersecurity trends and scenarios. The key tasks of this ad hoc working group include:

- advising and contributing to ENISA's foresight methodology for cybersecurity long term scenarios;
- advice on interdisciplinary systems and long-term thinking, long-range planning, systematic trend watching, scenario development, and visioning;
- review of related ENISA deliverables;
- advice ENISA stakeholders, decision- and policymakers on emerging opportunities, risk management and appropriate mitigation strategies; and
- generally advising and contributing to carrying out ENISA's tasks in relation to foresight in cybersecurity.

1.4 METHODOLOGY

In line with ENISA's foresight framework, a structured seminar/thematic workshop was organised with key stakeholders to review the findings of the 2030 Report. Prior to the workshop we used a Real-Time Delphi survey technique to engage stakeholders in the initial review of threats for 2030 (Chapter 3).

The Delphi technique is a structured and iterative method used to gather collective forecasts and expert opinions on likely or possible developments in specific areas. It aims to derive valuable insights from a group of experts while avoiding the biases and limitations associated with group dynamics and dominant individuals. Delphi Surveys can be carried out face to face, online or by post. In online versions, participants are given their own login and password to access the site. The process typically involves multiple rounds of questionnaires, feedback, and refinement, leading to a convergence of opinions or the identification of a wide range of potential developments. Inputs were collected during the two weeks leading to the workshop. We invited 33 experts, out of which 24 took part in the exercise, logging at least once, and 13 were highly active, logging more than twice and filling out the entire survey, as well as providing comments. The real-time Delphi survey was active from September 25th until October 10th.

The thematic workshop was held online on 12 October 2023 and gathered a group of 10 experts and practitioners who worked out the possible changes in trends' trajectories and reconciled their final findings on the scenarios. The workshop consisted of two parts:

- Session reviewing 2030 trends (Chapter 4)
- Review of scenarios based on the outcomes of previous steps.

To ensure a quality review we have conducted a validation process of the report utilising expertise of Ad hoc Working Group on Foresight for Emerging and Future Cybersecurity Challenges, as well consulting the ENISA National Liaison Officers network and the Advisory Group composed by experts from industry, academia, business, and consumer groups, as well as nominated members AG. By involving wide range of stakeholders from both state and non-state sectors, we have made sure that all the findings have been verified and crosschecked but more importantly that they are relevant.

The results of the review process are further presented in this report through sections that are dedicated to each of the process segment:

- Threats: this section will provide information on the results of the real-time Delphi.
- Trends: this section will provide information on the results of the workshop dedicated to review the trends through the lens of possible disruptions, further inflating or deflating the trends selected by workshop participants
- Scenarios: this section will provide information on the experts' feedback to original ENISA 2030 scenarios, including their revised versions.

2. THREATS

The threats were revised during an online real-time Delphi survey. Twenty-four experts contributed to the survey, adding their assessments of threats' impact and likelihood, as well as numerous comments substantiating the provided assessments. The real-time Delphi survey resulted in formulation of a revised top ten list of threats, based on their impact and likelihood scoring multiplication:

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]**

Two trends were excluded from the top 10 list: **Lack of Analysis and Control of Space-based Infrastructure and Objects**, and **Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data.**

Two trends moved up from lower positions to be included in the 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**.

2.1 SUMMARY

The threat prioritisation based on [impact * likelihood] assessment is presented in the table below, starting with the most prioritised.

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

The Delphi survey reveals a dynamic landscape of cybersecurity threats with both perceived impacts and likelihoods of various threats changing between 2022 and the projected scenario in 2030. Notably, "**Supply Chain Compromise of Software Dependencies**" has seen a decrease in both impact and likelihood, indicating potential improvements in supply chain security measures. Nevertheless, it remains a significant concern, ranking high in terms of risk, with a score of 17.71.

The rise of "**Advanced Disinformation/Influence Operations (IO) Campaigns**" is predicted to have a decreased impact and likelihood, possibly reflecting increased efforts in countering disinformation campaigns. However, it remains a substantial threat, ranking at 14.38. "**Rise of Digital Surveillance Authoritarianism/Loss of Privacy**" also showcases a slight decline in impact but a significant drop in likelihood, possibly indicating growing privacy-consciousness in the coming years, though it still ranks high at 15.34.

Some threats, such as "**Skill Shortage**" and "**Cross-border ICT Service Providers as a Single Point of Failure**," have seen increases in impact, signifying their growing significance, with rankings of 17.20 and 15.12, respectively. Additionally, "**Abuse of AI**" has seen an increase in likelihood, suggesting the potential for AI-driven cyberattacks, while "**AI Disrupting/Enhancing Cyber Attacks**" shows a similar trend. Meanwhile, optional threats like "**Increased Digital Currency-enabled Cybercrime**" and "**Exploitation of Unpatched and Out-of-date Systems Within the Overwhelmed Cross-sector Tech Ecosystem**" have emerged with noteworthy rankings at 10.25 and 16.21, respectively.

Consensus, measured by the Standard Deviation of answers, is covered later in the subsequent chapter.

Additionally, the participants proposed four novel threats that could be considered in the revision process. They are quoted below verbatim, with only minor spelling and grammatical changes to improve perusal:

1. **Overreach in Trust Towards Algorithms.** People will "believe" the computer too much. If chat GTP or google says this or that, then it's true. https://news.ycombinator.com/item?id=37145312 (I tried it out myself with google

about two weeks ago it worked at that time, but no longer). I had to show a student a law text, because he was believing a google answer more than mine (that was about some EU fines).

2. **Historic Risk Management Fallacy.** Probabilistic approaches to threat detection will cause blind spots in cybersecurity because they are derived from identifying current threats and rating their likelihood of increase or decrease. The adoption of these methods will limit cybersecurity actors' ability to perceive new threats which emerge from outside the current frame of reference. This threat's impact or likelihood is increasing, precisely because of the task we are currently undertaking - and the approach here should be complemented by other approaches which encourage strategic reframing. See the Information Security Forum and their new version of THREAT HORIZON for an example of a preferable approach.
3. **Emergence of Metaphysical Relationships with AI**. There will be a growing number of people who will identify with AI's. From considering it a pet to those who think it is a god.
4. **Disruptions within the EU Intelligence Community.** "We must be very cautious in addressing intelligence sharing at the EU level and tackling hybrid threats. I wanted to comment on the relevant question (n°2), but the platform was acting up, so I am putting it here: we need to come together on these topics because they are the two faces of the same coin. Intelligence sharing provides a shared situational awareness but must happen within a properly defined framework mindful of bureaucratic hurdles. Hybrid threats are multifaceted by definition and must clearly include information disorders. The latter is a way more appropriate to express the modulation of information by adversarial actors (compared to dis-/misinformation, fake news, etc.). Failing to address these profound changes in a systemic matter is a threat."

2.2 DETAILED ANALYSIS OF DELPHI RESULTS

2.2.1 Evolution of assessments between 2022 and 2023

The table below articulates the evolution of assessments between the original report and the Delphi study. Only a few significant changes are observed. The only threats that had their impact rating published in the report are considered. The perceived changes of impact and likelihood from Delphi participants reflect their consensus, as the likelihood of these future events is not based on historical occurrence or other statistical grounds.

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▼**

2.2.2 Comments

All comments provided by the real-time Delphi survey participants are provided in Annex 1.

2.2.3 Consensus rating based on the standard deviation of assessments

Standard deviation is a statistical measure that quantifies the amount of variation or dispersion in a set of values. In the context of surveys, standard deviation is useful in understanding consensus among respondents, as a measure of agreement or disagreement.

A low standard deviation indicates that the responses or data points tend to be very close to the mean, suggesting a high level of agreement or consensus among the respondents.

Conversely, a high standard deviation indicates that the responses are spread out over a larger range, which means there might be a lack of consensus or agreement among respondents. In this real-time Delphi survey, the final standard deviations show a low dispersion, which is evocative of consensus among the experts.

"**Skill Shortage**" showcased one of the lowest standard deviations in likelihood assessments at 0.44. Similarly, the "**Rise of Advanced Hybrid Threats**" had a low variation in its likelihood with a standard deviation of 0.51. "**AI Disrupting/Enhancing Cyber-attacks**" and "**Exploitation of Unpatched and Out-of-date Systems Within the Overwhelmed Cross-sector Tech Ecosystem**" followed with standard deviations of 0.54 and 0.58 for their respective likelihood assessments.

The "**Supply Chain Compromise of Software Dependencies**" reported a standard deviation of 0.72 for its likelihood. In comparison, "**Abuse of AI**," "**Attacks Using Quantum Computing**," and "**Targeted Attacks (e.g. Ransomware) Enhanced by Smart Device Data**" presented likelihood standard deviations of 0.79, 0.70, and 0.71 respectively. "**Lack of Analysis and Control of Space-based Infrastructure and Objects**" indicated a standard deviation of 0.67 in its likelihood.

"**Exploitation of E-health (and Genetic) Data**" displayed a maximum standard deviation of 1.00 for likelihood, indicating considerable uncertainty or diversity in assessments. Following closely were threats like **"Advanced Disinformation / Influence Operations (IO) Campaigns"** and **"Rise of Digital Surveillance Authoritarianism / Loss of Privacy"** with likelihood standard deviations of 0.88 each.

Moving to the impact assessments, while threats such as "**Skill Shortage"** and "Rise of advanced hybrid threats**"** demonstrated relatively low variations, other concerns like the "Cross-border ICT service provider as a single point of failure" and "**Exploitation of e-health (and genetic) data**" reported higher variations, with standard deviations of 0.91 and 0.94 respectively.

3. TRENDS

During the workshop the experts present were asked to indicate which of the trends described in this report is more likely to be altered than others and to provide specific ideas about the direction of change - given trends were speeding up or collapsing by 2030. Nine trends (described below, also see Annex 2) were selected by workshop participants for discussion based on their conjoint vulnerability to change, either positive, (i.e., a given trend to intensify) or negative, as well as their importance to cybersecurity. These nine trends were then discussed by the participants in a facilitated, structured discussion using the 4CF Stranger Futures workshop method. These nine trends are susceptible to change in the next seven years which may affect the way and intensity in which they impact cybersecurity threats.

- 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.

For the better understanding, however, we encourage you to refer to graphs on the Annex 2.

All these trends, with one exception, were, after an exchange of arguments for and against, rated as speeding up beyond their dynamics originally presented in ENISA 2030 Threats Foresight Report. The exception concerns social trend of Decision-making being increasingly based on automated analysis of data. Experts could not reach a consensus as to whether this dynamically evolving trend is moving faster or slower and they noted ambiguity of its projected development.

As much as the experts expressed concern about the way that these trends affect cybersecurity, in several examples they anticipated EU regulations to specifically address their negative influence.

3.1 POLITICAL TRENDS

3.1.1 Increased political power of non-state actors

The trend of increasing global interconnectedness is expected to speed up even further, and consequently facilitate interactions among non-state actors, often surpassing the state's ability to regulate them. This phenomenon suggests a decline in the influence of nation-states, particularly in their control over these evolving forms of interactions. Non-state actors, who are less bound by regulations and can adapt more swiftly, tend to have access to similar tools as state actors. State actors, constrained by more rules and frameworks, may operate at a slower pace. While there is an observable increase in non-state actor influence, it is worth noting that the state's authority in this context was historically limited. Some experts see positive elements in the state's attempts to reintroduce itself and implement rules and regulations, even though a substantial power gap exists. Additionally, the use of cyber diplomacy tools and initiatives to safeguard national interests and promote security cooperation in dealing with cross border and international cyber threats is seen as a positive force striving to mitigate the adverse consequences of this trend.

3.1.2 The increasing relevance of (cyber) security in elections

The growing significance of (cyber) security in elections is a notable trend expected to grow even further. Experts have pointed out the various aspects, including the rising threat of interference through hybrid attacks, social engineering tactics, and the dissemination of disinformation to manipulate voters. There is also an emphasis on the capacity to create more sophisticated disinformation materials/campaigns and the profiling of voter's preference particularly through the existing or new social networks that are seen less regulated from the prospective of election regulators. These concerns are particularly relevant during electoral debates and campaigns, where the influence on campaigns is a shared thought among experts. It's worth noting that while campaigns may experience less direct attacks on their infrastructure, the most concerning aspect is the potential for long-term influence, even before official campaigns, driven by precise profiling techniques.

3.2 ECONOMIC TRENDS

3.2.1 Collecting and analysing data to assess user behaviour is increasing, especially in the private sector

The trend of collecting and analysing data to assess user behaviour is on the rise. This entails using data for automated decision-making processes, primarily aimed at enhancing customer targeting and reducing operational expenses. Additionally, there's a growing emphasis on the increasing digitalisation of various aspects of life and the advancement of AI algorithms.

However, experts highlight several concerns and considerations within this trend. These include the potential limitations of behavioural analysis, such as the influence of technology and context on behaviour, leading to the need for accurate and context-aware analysis. Generalisation in behavioural profiling may result in inaccuracies and biases, despite the advantages of context-aware AI analysis.

Furthermore, while data collection is expected to continue increasing for some time, there's speculation that it may eventually reach a plateau or even decline as the limitations of data-driven models become apparent. Additionally, there are concerns about individuals adapting their behaviour to manipulate behavioural analysis, potentially leading to inaccurate results.

3.2.2 Increasing reliance on outsourced IT Services

The trend of increasing reliance on outsourced IT services is leading to a growing number of interactions in the digital landscape. This increased complexity of IT and IT-based processes is expected to continue for a significant period, posing challenges, especially for small and medium-sized enterprises (SMEs) that may struggle to manage these complexities independently.

There is a consensus among experts that this trend is valid and growing, acknowledging the difficulties in keeping these interactions safe. However, there is also concern about the potential consequences of this reliance on a limited number of non-EU cloud providers and the increased use of generative AI, primarily from US-based or non-EU providers. While regulations within the EU may attempt to address these issues, there's a potential trade-off between increased regulation and its impact on innovation and functionality in the IT outsourcing landscape.

3.3 SOCIAL TRENDS

3.3.1 Decision-making is increasingly based on automated analysis of data

The trend of decision-making increasingly relying on automated data analysis seems ambiguous to the experts. Concerns have been raised regarding the quality and safety of public data, often driven by the rush to bring products to the market quickly. This complexity in decision-making is leading managers to become reliant on automated systems, altering the nature and scope of accountability.

In this context, the focus has shifted towards what can be quantifiably measured, potentially neglecting the importance of making the right decisions. Most recent research showed that the use of automated analysis of data in areas related to social or public policy issues reduces decision making reliance on algorithmic advice relative to human advice and contextual understanding. Additionally, there is a risk of incorporating uncorrelated data into AI systems, resulting in undesirable outputs. The convenience of attributing suboptimal decisions to the system itself can also lead to a lack of accountability and responsibility in decision-making processes. On the one hand, this trend is powerful, however, on the other hand there are clear pitfalls that can be anticipated.

3.4 TECHNOLOGICAL TRENDS

3.4.1 The number of satellites in space is increasing and thus our dependency on satellites

The increasing criticality of satellite control infrastructure is driven by several factors. Critical infrastructure operations are shifting to orbit due to the advantages of the vacuum environment. However, this has raised concerns about traffic congestion in space and potential ecological challenges affecting the ozone layer, although some arguments against this notion have been considered dubious.

To address potential incidents, there are efforts to establish redundant networks in orbit. Nevertheless, the lack of adequate regulations over the private sector in space raises concerns. The decreasing importance of landlines, coupled with the growing number of space stations, necessitates greater coordination among them.

Public interest in space is leading to the proliferation of satellites, particularly for earth observation, which has become critical in monitoring climate-related catastrophes. Moreover, the use of satellites in the war in Ukraine may prompt the deployment of more military satellites.

However, this increased satellite presence also raises cybersecurity concerns. Satellite cybersecurity is perceived as weak, primarily due to the reliance on older cryptography methods, and operators are often reluctant to update their systems.

3.4.2 Vehicles are becoming increasingly connected to each other and to the outside world and less reliant on human operation

The trend of vehicles becoming increasingly connected is rising dynamically and it is driven by various factors. Car manufacturers see added benefits in enhancing connectivity, but car owners may have reservations about constant surveillance. As complexity in vehicle systems continues to rise, electric vehicles (EVs) with automatic charging contribute to increased connectivity.

The trade-off between increased safety and potential privacy concerns is a key aspect of this trend. While some argue that increased safety justifies the connectivity, others question whether the safety gains have been definitively proven.

In some cases, internal networks in cars that were meant to be isolated end up communicating, which amplifies complexity and exposure to potential risks. Additionally, there's a shift towards institutional vehicles gaining popularity over individual cars, with a focus on higher cybersecurity measures.

The diffusion of technology from premium cars to regular cars also plays a role in driving this trend, although there may be inertia in adopting these changes.

3.5 ENVIRONMENTAL TRENDS

3.5.1 The increasing energy consumption of digital infrastructure

Experts at first agreed that the current trend suggests that there is a significant increase in data volumes, driven by advancements in analytics and improved connectivity. This surge in data consumption is leading to a substantial rise in energy usage. Several factors contribute to this trend, including the growing use of AI and quantum computing, which are expected to be more widely available, driving even higher energy demands. Additionally, blockchain technologies and the energy efficiency of equipment are playing roles in this scenario. Despite potential improvements in energy efficiency through quantum and AI technologies, it is uncertain whether we will be fully prepared for the associated challenges by 2030. Furthermore, the growth of the internet is expected to slow down, but the existing infrastructure may not expand adequately. The development of smart cities could enhance energy efficiency, but there is a lack of consistent regulations across different technology layers, which could pose challenges. Overall, while there is optimism about solving issues related to renewable energy supply by 2030, there are concerns about the physical network's capacity for transmission. In the end however, from foresight perspective, the anticipation of a major energy breakthrough in the coming years rose to prominence in the discussion, calling into question the long-term viability of this trend.

3.6 LEGAL TRENDS

3.6.1 The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult

This trend was particularly problematic, as its assessment relies on the conjunction of two factors. Overall, the capacity to control data about oneself is facing several challenges in the evolving digital landscape. As the number of data points continues to increase, individuals are experiencing a decrease in their ability to control their own data. This is further exacerbated by the growing complexity of data systems.

Moreover, the general population often remains indifferent to data control until they encounter a specific issue or incident. As people age, they may find it increasingly challenging to control their data in legacy systems, with limited access to data controllers or administrators. In some cases, data administrators may not even have a clear understanding of the whereabouts of the data they manage, adding to the complexity of the situation. This lack of control over personal data is driven by various factors, including the proliferation of data in the networked world and the potential benefits of Big Data. Societal priorities, such as addressing climate crises and conflicts, may shift the balance between individual autonomy and collective safety, potentially impacting data control.

Federated identities are emerging as a solution that simplifies data management. However, in the absence of public interest, regulators may resort to automated solutions with minimal opposition. Non-state actors, such as banks, can also play a role in shaping data control practices. Sensitive data and privacy concerns are expected to gain more attention as the volume of sensitive information grows. The fear of embarrassment due to compromised data may drive individuals to care more about data control. However, the definition of sensitive or private data may evolve over time, and what is considered shameful may change.

Ultimately, the control of personal data may become contingent on the policies and practices of data collectors and holders, with some powerful players potentially limiting access to services for those who do not agree with their terms and conditions. The dynamic nature of data control highlights the need for ongoing discussions and regulatory considerations.

4. SCENARIOS

The experts' revisions across the scenarios convey a critical viewpoint, emphasising concerns regarding trust, privacy, technology misuse, and environmental consequences. They advocate for more specific and nuanced scenarios to be redrafted, which will comprehensively explore the potential outcomes of technological advancements. In Scenario 2, the suggested changes provide a detailed perspective on challenges linked to water scarcity, technological reliance, and non-state actors' roles. Scenario 3 highlights the need to consider both positive and negative aspects of data-driven decision-making, ethical dilemmas, trust issues, and encryption's effects on law enforcement. The revisions in Scenario 4 delve into decentralisation in energy generation, automation in agriculture, and cybersecurity challenges due to evolving work structures. Furthermore, they underscore the impact on innovation, competition, and EU competitiveness. Lastly, Scenario 5 introduces additional factors, including the potential internet fragmentation, climate-related challenges, EU control measures, AI and data sovereignty challenges, and the role of space technologies in dependencies and vulnerabilities.

According to the experts' opinion, implementation of these revisions into the scenarios will better serve the purpose of stimulating strategic thinking and helping to overcome the limitations of thinking facing ambiguity and complexity.

As part of the review, we received comments during the workshop to make scenarios more specific and underline the challenges. We include the comments in extenso, testament to specific and often highly engaged feedback from the participants of the workshop.

4.1 SCENARIO 1 – BLOCKCHAIN, DEEPFAKES, & CYBERCRIME IN A DATA-RICH ENVIRONMENT

Experts suggest some modifications, including addressing concerns about trust, privacy, and the misuse of technology. Below is a summary of the suggested changes:

- **Blockchain's Widespread Use:** While the original text highlights blockchain's widespread adoption in various sectors, the experts have questioned its ubiquity, raising doubts about its significance in some scenarios and suggesting the need to consider other potential use cases.
- **Criminal Exploitation of Technology:** Experts emphasise that criminal groups are using advanced technology, including distributed ledger technology (crypto) and the darknet, to expand their activities. This is seen as contributing to a constant battle for security, erosion of state power, and the need for alternative enforcement mechanisms.
- **Deep Fake Technology:** The original text mentions the mainstream use of deep fake technology and its impact on education, art, and entertainment. Experts highlight concerns about the psychological effects of deep fakes, including the erosion of trust and the spread of paranoia.
- **Privacy and Data Analysis:** The text discusses how organisations rely on real-time analysis of customer data for various purposes. Experts suggest emphasising the commercial data validation activities and the changing landscape of trust in data.
- **Data Collection and AI:** While the original text discusses the collection and analysis of data from infrastructure components using AI, experts raise questions about the environmental impact of tech "waste" and the potential interference of deep fakes in managing AI-empowered infrastructure.

4.1.1 Updated scenario

By 2030 **blockchain technology** has indeed witnessed widespread adoption across various sectors, and its potential applications continue to expand. However, it's important to recognise that blockchain is not a one-size-fits-all solution, that raises valid questions about its ubiquity and significance in certain scenarios. One of the primary concerns surrounding blockchain's widespread use is its efficiency and scalability. In some cases, traditional centralised systems may outperform blockchain in terms of speed and cost-effectiveness. For instance, high-frequency trading in financial markets demands sub-millisecond transaction times that many blockchain networks cannot currently provide. This leads to questions such as whether blockchain is the right choice for all financial applications.
Additionally, while blockchain offers transparency and immutability, it may not be the best solution for every data privacy requirement. In situations where complete anonymity and privacy are paramount, other technologies or approaches may be more suitable. Despite these concerns, blockchain's significance remains undeniable in various sectors.
The **criminal exploitation of advanced technology**, including distributed ledger technology (commonly associated with cryptocurrencies) and the darknet, is a growing concern for law enforcement and security agencies worldwide. These developments have significant implications for security, governance, and the need for alternative enforcement mechanisms.

- Criminal organisations are increasingly using cryptocurrencies like Bitcoin for money laundering and other financial activities. The “pseudonymous” nature of these digital currencies makes it challenging for authorities to trace transactions and identify the parties involved. This has led to concerns about the erosion of financial oversight and the ability of governments to combat money laundering and illicit financial flows.
- The darknet, a part of the internet that is intentionally hidden and only accessible through specialised software, has become a hub for illegal activities, including the sale of drugs, weapons, and stolen data. Law enforcement agencies struggle to monitor and regulate these hidden online marketplaces, making it difficult to combat criminal activities effectively. Furthermore, the borderless nature of the internet allows cybercriminals to operate from anywhere, making it challenging for law enforcement to apprehend them.
- The use of strong encryption to protect communications and data can also hinder law enforcement's ability to intercept and access criminal communications. While encryption is essential for protecting individual privacy and data security, it poses challenges for lawful surveillance in criminal investigations.
- The rise of technology-driven criminal activities has prompted discussions about the need for alternative enforcement mechanisms. Some have proposed stronger international cooperation, updated legal frameworks, and increased investments in cybersecurity and digital forensics to combat these evolving threats effectively.

In this landscape, there is a constant battle for security, with law enforcement agencies and governments adapting their strategies and tools to address the challenges posed by criminals exploiting advanced technology. Balancing the need for privacy and security in the digital age remains an ongoing challenge, and the development of effective policies and practices is essential to mitigate the negative impacts of technology-enabled criminal activities.

In addition, the mainstream use of **deep fake technology** has indeed expanded its influence across various sectors, such as education, art, and entertainment. However, valid concerns were raised about the psychological and societal effects of deep fakes, including the erosion of trust and the spread of paranoia.

- **Erosion of Trust**: Deep fakes, which involve the use of artificial intelligence to create hyper-realistic but entirely fabricated content, can erode trust in visual and audio media. When people can no longer rely on what they see or hear, it becomes increasingly challenging to discern fact from fiction. This erosion of trust can have significant consequences in domains where trust is paramount, such as journalism and law enforcement.
- **Manipulation and Misinformation:** Deep fake technology can be used to manipulate images and videos, potentially leading to the spread of misinformation. In politics, for example, deep fakes could be used to create convincing videos of public figures saying or doing things they never did. This can have far-reaching consequences for public discourse and decision-making.
- **Paranoia and Disbelief:** As deep fake technology becomes more sophisticated and accessible; it can lead to heightened levels of paranoia and disbelief. People may question the authenticity of any media they encounter, which can impact their ability to make informed decisions and engage with content in a meaningful way.

While deep fake technology has made notable advancements in education, art, and entertainment, its potential for misuse and the associated psychological and societal impacts are significant.

While real-time analysis of customer data is invaluable for organisations for a wide range of purposes, including marketing, product development, and customer service, it's imperative that they place a strong emphasis on **commercial data validation activities** to ensure data quality, privacy, and security. Building and maintaining trust in data is becoming a fundamental aspect of business operations, and organisations that excel in this regard are more likely to succeed in the digital landscape.

The **collection and analysis of dat**a from **infrastructure components using AI** offer significant benefits in terms of efficiency, maintenance, and overall performance. However, this raises legitimate concerns about the environmental impact of tech "waste" and the potential interference of deep fakes in managing AI-empowered infrastructure. For example, the rapid pace of technological advancement and the shorter lifespans of electronic devices contribute to a growing problem of "e-waste", which includes discarded hardware and equipment, therefore sustainable and responsible disposal practices are essential to mitigate this issue.
Furthermore, deep fake technology, which uses AI to manipulate images and videos, can pose a significant challenge in the context of managing AI-empowered infrastructure. Malicious actors could use deep fakes to create convincing but false videos or images, potentially disrupting the monitoring and decision-making processes of critical infrastructure management systems.
Addressing these issues requires a combination of sustainable technology practices, strong cybersecurity measures, and ethical considerations to ensure the responsible and effective use of AI in infrastructure management.

4.2 SCENARIO 2 – ECO-FRIENDLY, SUSTAINABLE, AND INTERCONNECTED SMART CITIES (NON-STATE ACTORS)

Experts suggest some modifications, including addressing concerns about making this scenario different from the 1st one and going deeper and more specifically on some of this scenario's traits:

- **Water Scarcity Challenges:** While the original text discusses challenges posed by water scarcity in 2030 due to population growth and climate change, experts suggest considering the impact of water scarcity on global tech production. They also note that critical resources, such as water, will become less available, emphasising the reliance on satellite observation.
- **Impact on Living Costs:** Experts mention the potential consequences of water scarcity, including low-energy use, climate and economic shocks, austerity measures, and activity halts. They highlight the need for frugal technology use and digitally mediated cooperation to mitigate these challenges.
- **Role of Smart Cities**: The experts support the idea of smart cities and regions making better decisions about public resources like water and energy. However, they caution that increased technological integration in cities may lead to technological dependence and discuss the role of tech giants like Google in city development.
- **Political Power of Non-State Actors:** The original text mentions the growing political power of non-state actors, and experts seek clarification on whether this includes non-national public sector entities. They anticipate billionaires taking a significant share of unregulated sectors and emphasise the potential for a more participatory future depending on cultural context.
- **Digital Communities and Telecom Providers:** Experts note that digital communities and institutions are beyond the control of the state and influence all levels of governance. They question the level of trust in tech giants like Google. Additionally, they highlight the importance of telecom providers, not just due to new technology but as critical infrastructure operators.

4.2.1 Updated scenario

Water scarcity is indeed a significant challenge that is expected to intensify by 2030 due to factors like population growth and climate change. This is a multifaceted challenge that affects not only agriculture and human populations but also critical industries like tech production. The technology industry is highly water-intensive, particularly in the manufacturing processes of semiconductors and other electronic components. Water scarcity can disrupt supply chains, increase operational costs, and affect the availability of critical materials for tech production. To address these challenges, a combination of water-efficient technologies, global collaboration, and satellite observation for resource monitoring is essential to ensure the sustainable use of this vital resource.

Furthermore, water scarcity can indeed have far-reaching consequences, including **effects on living costs**, energy use, climate, and the economy. For instance, it can lead to increased living costs, particularly in regions where water is in short supply or to reduced energy production, especially in regions where hydropower is a significant energy source. Water scarcity is also closely linked to climate change, as it can lead to droughts and shifts in weather patterns. These climate shocks can disrupt agriculture, lead to crop failures, and impact food prices. In turn, these disruptions can lead to economic shocks that affect jobs, industries, and overall economic stability.
To mitigate the impact of water scarcity, adopting **frugal technology** could be a solution, which involves developing and using technologies that are more resource-efficient and environmentally sustainable. This can apply to both individual consumers and businesses, promoting responsible use of water and other resources. Furthermore, **digital technology** can also play a crucial role in managing water scarcity by enabling more efficient monitoring and management of water resources.

The concept of **smart cities** and regions holds promise in enabling better decision-making and resource management, such as for water and energy. It has the potential to revolutionise urban living and resource management, but it also brings challenges related to dependence on technology, data privacy, and equity. Relying heavily on technology can make cities vulnerable to disruptions, whether due to cyberattacks, infrastructure failures, or technical glitches. Therefore, cities need robust contingency plans to address such vulnerabilities.
Therefore, balancing the benefits of technological integration with responsible governance and community engagement is key to realising the full potential of smart cities while mitigating potential downsides.

The growing **political power of non-state actors** is a complex and evolving phenomenon encompassing a wide range of entities beyond traditional nation-states. There is concern that some billionaires and ultra-wealthy individuals could amass substantial influence in unregulated or underregulated sectors, potentially circumventing traditional governmental structures. As this power dynamic evolves, it raises questions about accountability, equity, and the potential for more participatory governance models, all of which can vary depending on cultural and regional contexts.

The role of **digital communities** and institutions, along with tech giants in shaping governance and their influence on various levels of government is a significant development in the digital age. Trust, regulation, and the responsible use of power are central concerns. For instance, trust in technology companies like Google, Facebook, and others is a critical concern as these companies collect vast amounts of user data and have significant influence over the flow of information and communication. Meanwhile, telecom providers have evolved into critical infrastructure operators, with a growing focus on security, national interests, and digital inclusion. Their services are essential for communication, data transmission, and connectivity. As such, they play a vital role not only in supporting new technologies but also in ensuring the functionality of modern society. Balancing innovation and security in the digital age presents ongoing challenges for policymakers and society.

Furthermore, the impact on **election ecosystems** is a crucial aspect of discussions on technology and politics. For instance, the use of propaganda and hacking to discredit political actors is a significant concern in the digital age. Malicious actors can exploit technology to spread misinformation, interfere with elections, and manipulate public opinion. Addressing these issues requires robust cybersecurity measures, digital literacy, and fact-checking initiatives. Moreover, trust in local democracy is an essential element of any functioning political system. Therefore, there is a need to establish and maintain trust at the local level, as it forms the foundation of broader democratic processes. This can involve promoting transparency, civic engagement, and responsive governance in local communities. Technology could be used to both support and undermine local democracy. Therefore, leveraging technology to enhance local democracy and ensure the integrity of local elections is essential for the continued health of democratic processes.

4.3 SCENARIO 3 – MORE DATA, LESS CONTROL

Experts suggest some modifications, including addressing concerns about trust, norms, and their enforcement in different markets.

- **Data-Driven Decision-Making:** While the original text discusses the automation of data-driven decisions, experts suggest considering the potential increase in cyberattacks targeting automated decision-making systems. They also note that people may willingly delegate decision-making to machines when they feel less competent.
- **Ethical Challenges:** The experts highlight ethical challenges in sectors like medical diagnostics, autonomous vehicles, and finance due to data-based and automated decision-making. These challenges include potential discrimination, privacy violations, and threats to human self-determination.
- **IoT Device Challenges:** The original text mentions problems with patch management for organisations using IoT devices. Experts recommend better ways to measure trustworthiness of data and sources, especially when "hard" verification methods are not feasible. They emphasise the need for harmonising "hard" and "soft" trust assessments.
- **Data Breaches and Trust Issues:** Experts provide additional resources and links to emphasise the impact of data breaches, online bullying, and cyberbullying on public health and trust in the digital economy. They highlight how these incidents lead to reduced usage of digital products and services.
- **Concerns Over Data Usage:** The experts note that EU consumers are increasingly concerned about data usage and call for more control over data access and usage rights. They suggest that better infrastructure support for controlling data usage and enforcing consent could increase trust.
- **Complex Relationship with social media:** Experts have pointed out the complex relationship between the concerns about the quality or reputation of social media platforms and actual withdrawal from them. They cite examples of Facebook, TikTok, and Twitter to highlight the nuances of this relationship.
- **Law Enforcement Challenges:** The experts discuss challenges faced by law enforcement in accessing and using data due to end-to-end encryption, data privacy regulations, and technical limitations. They also provide a perspective on data protection regulations.

4.3.1 Updated scenario

The automation of **data-driven decision-making** has the potential to offer significant benefits, but it also brings about important considerations related to cybersecurity, human trust, ethics, data quality, and accountability. As organisations increasingly rely on automated decision-making systems, they become more attractive targets for cyberattacks. Malicious actors may attempt to manipulate or compromise these systems to achieve their own objectives. Furthermore, people may willingly delegate decision-making to machines when they feel less competent or when they believe that automation can lead to better outcomes. A thoughtful and balanced approach to automation, with a focus on transparency and collaboration, is essential to harness the full potential of these technologies while mitigating their associated risks.

As technology continues to drive data-based and automated decision-making across various sectors, addressing the associated **ethical challenges** is paramount. These challenges span from potential discrimination and privacy violations to concerns about transparency, accountability, and preserving individual self-determination. For example, automated decision-making systems can inadvertently perpetuate or exacerbate biases present in the data they are trained on. This can result in discriminatory outcomes, such as in medical diagnostics, where certain groups may receive less accurate or equitable treatment. Moreover, ethical challenges arise when individuals' ability to make choices and determine their own actions is constrained by automated systems. For example, in autonomous vehicles, decisions about safety and navigation may override individual preferences. Therefore, it's essential to prioritise ethics in the development and deployment of automated systems to ensure they benefit society while respecting individual rights and values.

Furthermore, **IoT devices** have become increasingly prevalent in various applications, but they also pose several challenges, particularly in the context of patch management, data trustworthiness (e.g.: healthcare monitoring, autonomous vehicles), and trust assessment. Harmonising "hard" and "soft" trust assessments is essential particularly, when "hard" verification methods, such as physical sensors, are not feasible. Therefore, organisations need to develop comprehensive strategies to address these challenges and ensure the secure and reliable operation of IoT systems.

Data breaches, online bullying, and cyberbullying indeed have far-reaching consequences for public health and **trust** in the digital economy. When individuals and communities experience data breaches or become victims of online bullying and cyberbullying, trust in digital platforms, online services, and social networks erodes. This reduced trust can result in people being less willing to use digital products, share personal information, or engage in online activities. Addressing these concerns involves a multifaceted approach that includes preventive education, policies, regulation, and cybersecurity measures to mitigate the risks and consequences associated with these incidents.

Addressing concerns over **data usage** and providing consumers with greater control over their data are essential for maintaining trust in the digital ecosystem. Individuals are increasingly aware of the value of their personal data and are concerned about how it is collected, stored, and used by organisations. Building better infrastructure to support control over data usage is therefore essential. This involves creating systems that allow individuals to easily manage their data preferences, including granting or revoking consent for data processing. Furthermore, consent management platforms and technologies can enable individuals to provide, withdraw, or modify their consent to data processing easily.

Moreover, the relationship between concerns about the quality or reputation of **social media platforms** and actual withdrawal from them is indeed complex, influenced by various factors. Users weigh various factors, including the platform's unique strengths and weaknesses, their personal needs and preferences, and the availability of alternatives. This complexity underscores the evolving nature of social media usage and individuals' decisions about how to engage with these platforms.

On the other hand, **law enforcement** agencies face multiple challenges when it comes to accessing and using data in a privacy-conscious and technologically advanced environment. Striking a balance between privacy and security, ensuring compliance with data protection regulations, and addressing technical limitations are essential for effective and ethical law enforcement practices in the digital age. Furthermore, the debate surrounding **encryption**, the **"going dark" myth**, and law enforcement's access to data is a complex one with valid arguments on both sides. While encryption is essential for protecting privacy and security, it does present challenges for law enforcement. Additionally, the potential impact of emerging technologies like quantum computing on encryption and data access adds an extra layer of complexity to the discussion.

4.4 SCENARIO 4 – SUSTAINABLE ENERGY, AUTOMATED/SHORT-TERM WORKFORCE

Experts suggest some modifications, including taking some of the scenario’s assumptions further, explaining the consequences.

- **Renewable Energy and IoT:** While the original text discuss the increased use of renewable energy and automation of equipment, experts suggest considering the possibility of a more decentralised control over energy generation by 2030. This shift could reduce the cybersecurity impact of IoT and infrastructure insecurities.
- **Agriculture Automation:** Experts note that automation in agriculture is not solely due to a lack of workforce but is a broader industrial trend. They mention possible dependence on a few agricultural ICT service providers as a cybersecurity concern. They also highlight the potential for evasive attacks in complex processes.
- **Food Security:** The exposure of agricultural infrastructure to a connected environment raises concerns about food security in EU countries.
- **Flexible Work Structures:** The experts suggest that the shortage of skilled workers may lead to challenges in cybersecurity skill development and a misbalance between advanced and elementary cybersecurity skills. They also point out potential consequences of the proliferation of short-term contracts, such as a gap between employers and employees, standardisation of corporate IT infrastructure, and an increase in outsourcing, which could increase the risk of hybrid attacks with a strong social engineering element.
- **Platformisation of Work:** Experts emphasise the extreme gap between high and low-educated individuals in the labour market due to the platformisation of work. They mention that this gap can affect innovation, competition, and competitiveness for the EU.
- **Everything-as-a-Service Model:** Experts suggest that the adoption of the everything-as-a-service model can lead to a proliferation of cyberattacks, particularly targeting easier targets. They mention that this could result from the proliferation of automated attack technology, generative AI, and outsourcing, along with salary inequality.
- **Dependency on Software Service Providers:** Experts highlight the potential impact on innovation, competition, and competitiveness for the EU due to the concentration of software service providers. They suggest that innovation could be driven by the possibilities and constraints of these software services.

Updated scenario

The integration of **renewable energy** and the automation of equipment are significant trends in the energy sector, however, the shift toward decentralised energy generation offers the potential to enhance resilience, reduce cybersecurity risks, and empower consumers by 2030. Decentralised energy generation can enhance the resilience of energy systems. For instance, in the event of natural disasters or other disruptions, localised energy sources can continue to function, providing power to critical infrastructure and homes. While decentralisation offers numerous benefits, there are challenges to address, such as grid management, energy storage, and regulatory frameworks. Furthermore, the continued integration of IoT technologies will play a critical role in managing these evolving energy systems effectively.

Automation in agriculture is driven by various factors, and it offers significant benefits in terms of efficiency and sustainability. However, it also raises important concerns related to data privacy, cybersecurity, and dependence on technology providers. For instance, attacks on automated farm equipment, data breaches, and other cyber threats can disrupt agricultural operations, compromise sensitive data, and lead to financial losses. Addressing these challenges requires a holistic approach that combines technological innovation, regulatory frameworks, and a focus on sustainable farming practices.

Furthermore, the increasing integration of connected technologies in agriculture offers benefits but also presents **food security** challenges. A breach or disruption in the agricultural sector can have cascading effects on the entire food supply chain. If connected infrastructure, such as automated farm equipment, processing plants, or transportation systems, is compromised, it can lead to delays in food production and distribution, impacting food availability and prices. To address food security concerns, it is crucial to build resilience into the agricultural sector such as the redundancy in critical systems, backup plans for technology failures, and strategies for managing and mitigating cybersecurity risks.

The impact of **flexible work structures** on cybersecurity is a multifaceted issue. Addressing the shortage of skilled workers, balancing cybersecurity skills, and managing the consequences of short-term contracts and outsourcing are vital for maintaining strong cybersecurity practices and defending against evolving cyber threats. Furthermore, the **platformisation of work**, characterised by the increasing reliance on digital platforms to connect workers with job opportunities, has indeed led to significant shifts in the labour market. High-skilled and well-educated individuals often have greater access to and success in the digital platform economy, while low-educated or less-skilled workers may find it challenging to secure stable and well-paying work through these platforms. To address the educational gap, it requires a concerted effort from various stakeholders to ensure that the benefits of the digital labour market are accessible to all individuals, regardless of their educational background. Therefore, reducing disparities and fostering inclusion in the digital economy can lead to a more equitable and competitive workforce for the EU.

The adoption of the **everything-as-a-service (XaaS) model**, which encompasses various cloud-based and subscription-based services, has brought numerous benefits but also raised cybersecurity concerns, given the automation of attack technology, generative AI, and outsourcing practices. For instance, the increased automation of attack technology, including the use of botnets and malware, has made it easier for cybercriminals to target a broad range of potential victims. Also, the use of generative artificial intelligence (AI) in cyberattacks can create more sophisticated and evasive threats such as crafting realistic phishing emails, mimic user behaviours, and adapt to security measures, making it challenging to detect and defend against such attacks. Furthermore, salary disparities in the cybersecurity industry can result in the recruitment of less experienced professionals by organisations with limited budgets. These less experienced individuals may be more vulnerable to social engineering attacks and less capable of defending against sophisticated threats. Addressing this challenge requires a comprehensive approach that combines education, robust security measures, threat intelligence sharing, and proactive defence strategies to protect organizations and individuals from evolving cyber threats.

Moreover, the **dependency on a limited number of software service providers** can have significant implications for innovation, competition, and competitiveness for the EU and other regions. When organisations heavily rely on a small set of software service providers, their innovation efforts may become somewhat constrained by the features, application programming interfaces (APIs), and integrations offered by these providers. As a result, organisations often innovate within the boundaries and possibilities of the software services they use. However, a high level of dependency can discourage organisations from exploring alternative or innovative solutions and can lead to market dominance by a few major players. To mitigate these risks and seize the benefits of digital transformation, it is crucial to foster a diverse and competitive digital ecosystem while promoting policies and measures that protect the EU's digital interests.

4.5 SCENARIO 5 – LEGISLATION, BIAS, EXTINCTIONS, & GLOBAL THREATS

Experts suggested changes along the following themes:

- **Urban Expansion and Fragmented Internet:** Experts suggest that by 2030, the internet may fragment into various platforms, potentially affecting global supply chains and digital sovereignty. They mention the possibility of the "Brussels effect" influencing digital supply chains, making them more aligned with EU values. They also point out potential climate-related challenges, such as energy supply disruptions affecting data centres and the need for resilient cloud services.

- **Disinformation and Authoritarianism:** In terms of foresight, experts recommend considering the social and political cohesion of the EU and the potential for authoritarian practices within member states. They emphasise the need to build controls into EU processes and cybersecurity infrastructure to mitigate the risk of member states compromising or misusing digital infrastructure.
- **AI and Data Sovereignty:** Experts highlight the challenges related to data ownership, sovereignty, data protection, and compliance arising from the use of AI-based systems, especially concerning algorithmic biases. They also point out biases related to age in cybersecurity, including issues affecting children, teenagers, and the elderly.
- **Space Technologies:** The experts express some scepticism about the relevance of the "space" angle in the scenario and its intricate link to the rest of the narrative. They suggest that space technologies and sovereign LEO constellations may affect critical services' resilience and interoperability, potentially creating space-based dependencies.
- **Dependency on Space-Based Infrastructure:** The experts raise questions about the probability of the "Kessler syndrome" scenario, which involves space debris. They also emphasise the vulnerability of Europe due to its dependence on space-based infrastructure for critical services, food production, and goods.

4.5.1 Updated scenario

The potential **fragmentation of the internet** and its impact on global supply chains, digital sovereignty, and climate-related challenges are important considerations in the context of **urban expansion** and the future of the digital landscape.

- Internet fragmentation, driven by varying regulations and regional standards, can lead to challenges in global supply chains. Companies may need to adapt their operations to comply with different digital rules in various regions, potentially increasing costs and complexity.
- As the internet fragments, countries and regions may assert greater control over digital technologies, data, and content. This can impact digital sovereignty, influencing how data is stored, processed, and governed, potentially leading to restrictions on cross-border data flows.
- The EU's regulatory choices can shape how digital supply chains operate globally, making them more aligned with EU values and standards ("Brussels Effect").

Furthermore, climate-related events, such as extreme weather conditions, can disrupt energy supply, potentially affecting data centres and the availability of cloud services. Therefore, ensuring a stable and resilient energy supply for digital infrastructure becomes crucial. Overall, addressing these challenges involves a combination of regulatory alignment, technological innovation, and sustainable practices to ensure a resilient and interconnected digital future.

The rise of **disinformation** and **authoritarian practices** is a significant concern in the digital age. Foresight efforts should be comprehensive, focusing on the social and political dynamics within the EU, the potential for authoritarian practices, and the establishment of controls to protect digital infrastructure. By proactively addressing these issues, the EU can work to preserve its democratic values and cybersecurity resilience in the face of evolving threats.

Moreover, the challenges related to **data ownership**, **sovereignty**, data protection, compliance, and algorithmic biases in the context of **AI-based systems** are significant concerns. For instance, AI systems can exhibit algorithmic biases that disproportionately affect certain groups or demographics. Ensuring fairness and accountability in AI algorithms is essential to avoid discriminatory outcomes and promote equitable decision-making. Consideration should be also given to age-related vulnerabilities in cybersecurity. For example, elderly individuals may face challenges in managing complex passwords, understanding phishing emails, and recognising fraudulent schemes. Addressing the challenges related to AI and data sovereignty, as well as age-related biases in cybersecurity, requires a multifaceted approach that combines robust data governance, algorithmic fairness, cybersecurity education, and targeted regulations to protect individuals across all age groups in the digital landscape.

While **space technologies** offer benefits such as global connectivity and data access, they can also introduce new points of failure. Space-based infrastructure, like satellites, can be vulnerable to space debris, solar radiation, and other space-related threats, affecting the resilience of services reliant on these assets. For instance, the deployment of sovereign Low Earth Orbit (LEO) constellations can create dependencies on space-based infrastructure for critical services. This introduces potential vulnerabilities and challenges related to system resilience and interoperability. Furthermore, **Europe's dependence on space-based infrastructure** for critical services, including telecommunications, navigation, and Earth observation, highlights the need for robust infrastructure resilience. Vulnerabilities can arise from disruptions to satellite networks, especially in the event of space debris collisions or space weather events affecting satellite functionality. Therefore, dependence on space-based infrastructure for food production, logistics, and goods delivery underscores the importance of diversification and redundancy in critical systems. Addressing the concerns related to space debris and Europe's vulnerability due to space-based infrastructure dependency requires a combination of international collaboration, infrastructure diversification, and proactive measures to mitigate risks and enhance resilience in critical systems.

ANNEX: GRAPHS

In the workshop an online tool was used to help the experts review trends. The tool that was used is a unique combination of the natural, intuitive flow of creative discussion with a structured tree of arguments, which helps to better understand complex topics and draw conclusions. The nature-inspired tree-like structure of the graphs generated during each session dynamically adapts to the development of the discussion.

In the most classical approach, discussion starts with a central topic - a certain trend, e.g., “Decision making is increasingly based on automated analysis of data”. Participants can then provide ideas for positive trend disruptions (“Trend will intensify, because…”) or negative trend disruptions (“Trend will collapse, because…”). The former is sometimes called hyper trends, and the latter anti-trends.

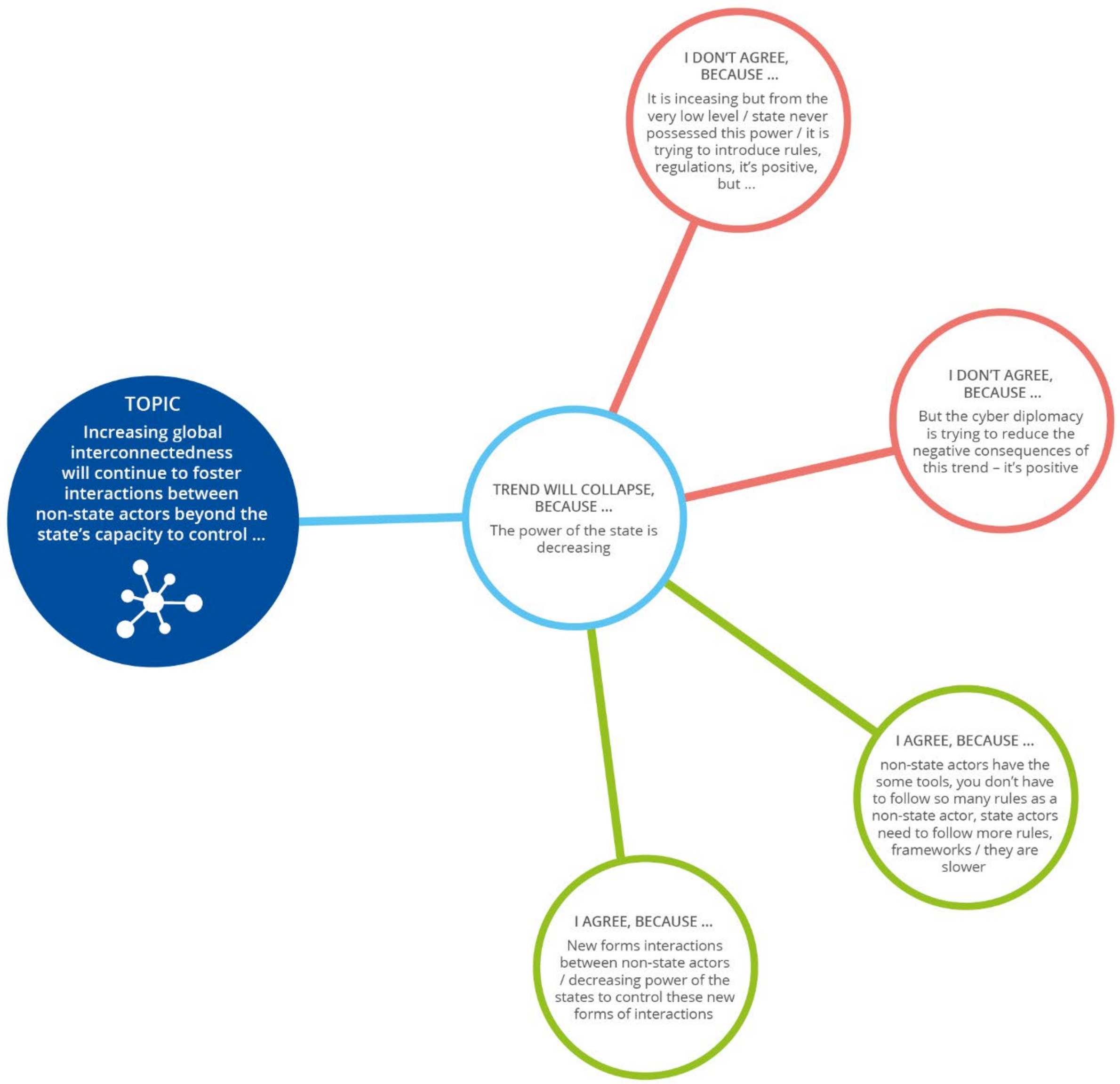
An example of a reason for potential trend intensification (hyper trend) can be the advent of quantum computing. On the other hand, the trend could theoretically collapse (anti-trend) due to new research that would expose the percentage of misguided decisions taken based on automated data analysis results. Participants can provide such ideas in comments (“nodes”), which are connected to the central topic. Furthermore, each idea can then be commented upon to express support or disagreement - rationale for these can be explained using additional nodes connected to the hyper trends and anti-trends and marked in green (agreement) or red (disagreement). Someone could use the red “disagreement” node to e.g., argue that quantum computing is still too early in development to be seriously considered, while someone else could express their support for the idea by providing information about the current progress in using quantum computing for enhancing data analysis.

The argument tree can be expanded indefinitely, by providing further arguments and ideas (either connected to the central topic, the hyper trends and anti-trends, or the supporting and opposing arguments). Participants can also use thumbs-up and thumbs-down buttons in each node, which impacts the user scores as well as the width of the connecting lines (“stronger” arguments have wider connectors).

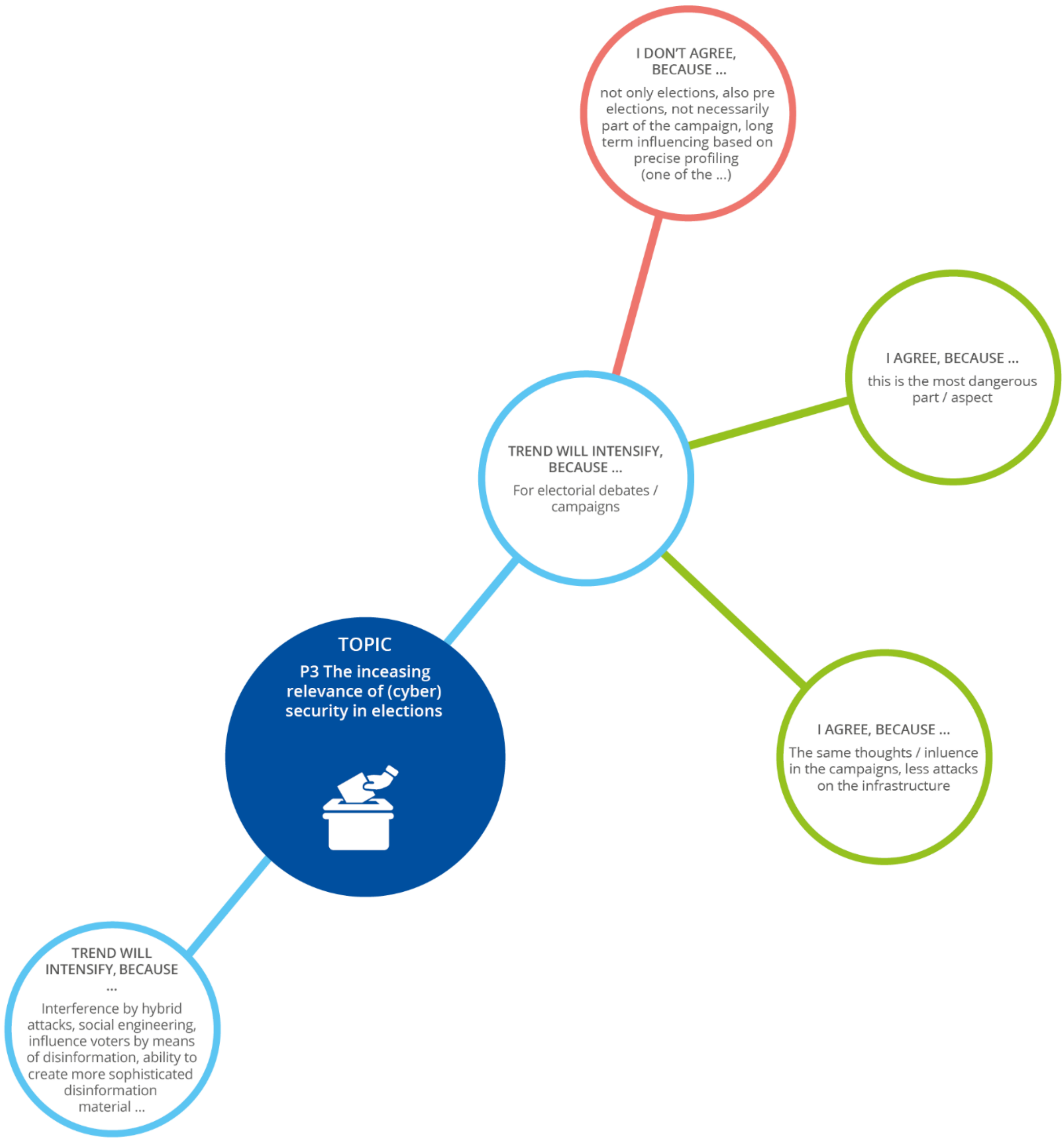
In the graph below we can see a part of a bigger argument tree, which focused on the trend used in the example above. We can see one idea for potential trend collapse, one idea for trend intensification, as well as two arguments supporting it.

Graph Environmental 8: Increasing energy consumption of digital infrastructure

Graph Political 2: Increased political power of non-state actors

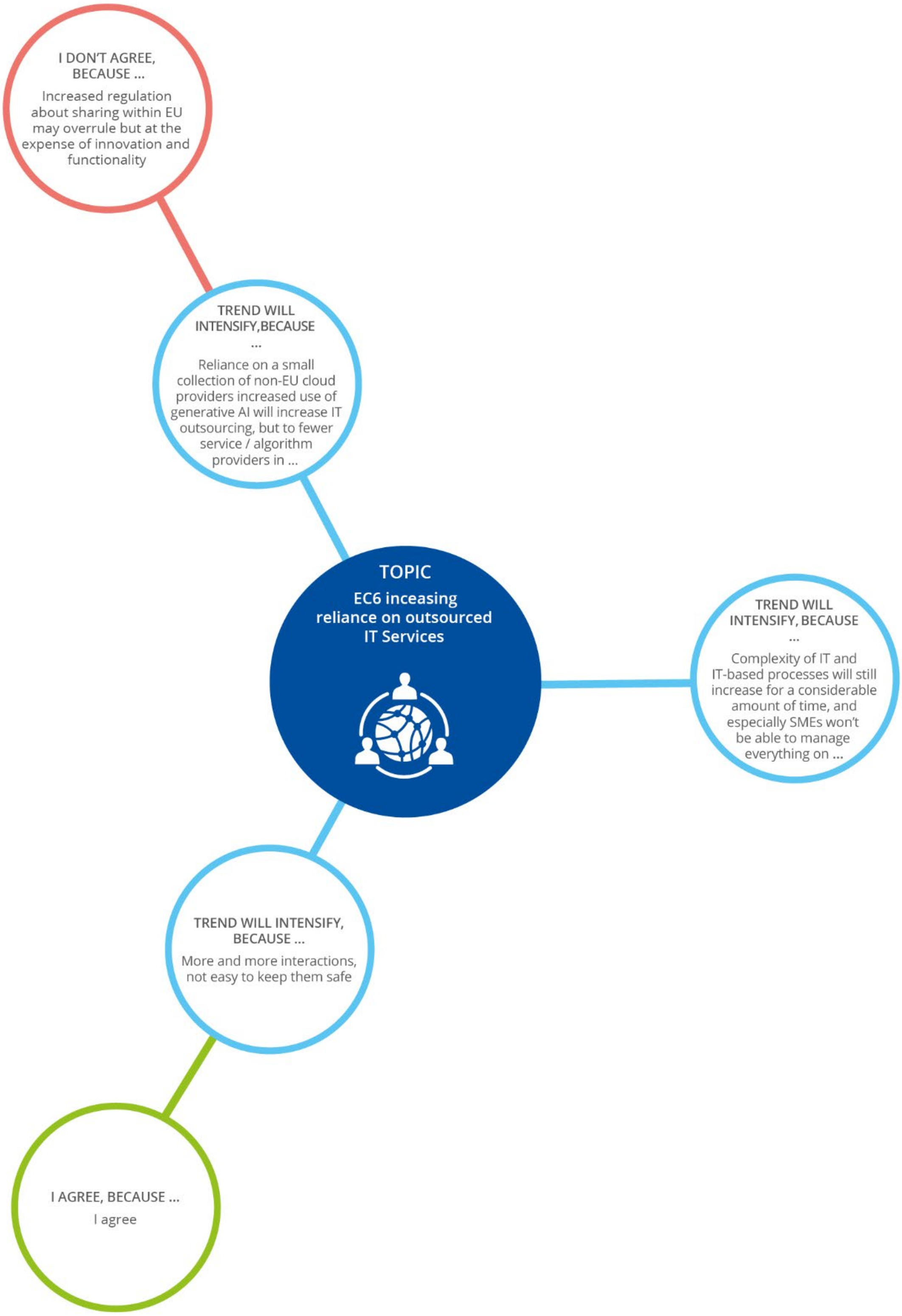


Graph Political 3: The increasing relevance of (cyber) security in elections



Graph Economic 4: Collecting and analysing data to assess user behaviour is increasing, especially in the private sector

Graph Economic 6: Increasing reliance on outsourced IT Services



Graph Social 2: Decision-making is increasingly based on automated analysis of data

Graph Technology 2: The number of satellites in space is increasing and thus our dependency on satellites

Graph Technology 5: Vehicles are becoming increasingly connected to each other and to the outside world and less reliant on human operation

Graph Legal 3: The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult

TP-02-24-509-EN-N

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

ISBN 978-92-9204-671-2
doi: 10.2824/349493