EUROPEAN UNION AGENCY
FOR CYBERSECURITY

IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030

MARCH 2023

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, boost the resilience of the Union's infrastructure, and, ultimately, keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use foresight@enisa.europa.eu
For media inquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Rossella Mattioli, Apostolos Malatras, - ENISA
Eve Naomi Hunter, Marco Gino Biasibetti Penso, Dominic Bertram, Isabell Neubert – Detecon

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.

1.1 LEGAL NOTICE

1.2 COPYRIGHT NOTICE

ISBN: 978-92-9204-634-7, DOI: 10.2824/117542

TABLE OF CONTENTS

2. INTRODUCTION 6

2.1 BACKGROUND 6

2.2 PURPOSE OF THIS EXERCISE 6

2.3 TARGET AUDIENCE 7

3. EMERGING CYBERSECURITY THREATS FOR 2030 8

3.1 SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES - #1 11

3.2 ADVANCED DISINFORMATION / INFLUENCE OPERATIONS (IO) CAMPAIGNS - #2 13

3.3 RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY - #3 13

3.4 HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBER-PHYSICAL ECOSYSTEMS - #4 14

3.5 TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA - #5 15

3.6 LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS - #6 16

3.7 RISE OF ADVANCED HYBRID THREATS - #7 17

3.8 SKILL SHORTAGES #8 18

3.9 CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE #9 19

3.10 ABUSE OF AI - #10 20

3.11 ADDITIONAL THREATS 21

4. 2030 TRENDS 24

4.1 PRIORITIZED TRENDS 25

1.1.1 Scenario 1 – Blockchain, deepfakes, & cybercrime in a data-rich environment 40
1.1.2 Scenario 2 – Eco-friendly, sustainable, and interconnected smart cities (non-state actors) 40
1.1.3 Scenario 3 – More data, less control 40
1.1.4 Scenario 4 – Sustainable energy, automated/short-term workforce 40
1.1.5 Scenario 5 – Legislation, bias, extinctions, & global threats 40

MAINTAINING AN EMERGING THREAT LISTING 41

4.2 DATA COLLECTION (AKA HORIZON SCANNING) 41

4.3 COLLABORATIVE ANALYSIS 41

4.4 SYNTHESIS 42

A METHODOLOGY 43

B FORESIGHT INFORMATION MODEL 45

B.1 TREND DESCRIPTION 46

B.1.1 Drivers of Change 47
B.1.2 Megatrends 47

B.2 THREAT ANATOMY MODEL 48

C TREND ANALYSIS 49

C.1 APPROACH & PROCESS 49

C.1.1 Expert Participant Analysis 50
C.1.2 Collaborative Exploration 50

D THREAT IDENTIFICATION 54

D.1 SCENARIOS 54

D.1.1 Scenario 1 – Blockchain, deepfakes, & cybercrime in a data-rich environment 54
D.1.2 Scenario 2 – Eco-friendly, sustainable, and interconnected smart cities (non-state actors) 55
D.1.3 Scenario 3 – More data, less control 56
D.1.4 Scenario 4 – Sustainable energy, automated/short-term workforce 56
D.1.5 Scenario 5 – Legislation, bias, extinctions, & global threats 57

D.2 SCIENCE FICTION PROTOTYPING (SFP) 57

D.3 THREAT PRIORITIZATION 58

E THREAT SCORING 59

5. BIBLIOGRAPHY 60

ABBREVIATIONS

Definitions related to cybersecurity and the European Union can be found on ENISA's website.[1]

AI	Artificial intelligence
APT	Advanced Persistent Threat
CISA	US Cybersecurity and Infrastructure Security Agency
GAN	Generative Adversarial Networks
CSIRT	Computer Security Incident Response Team
CSIRTs Network	EU CSIRTs Network of appointed CSIRTs
CyCLONe	EU Cyber Crises Liaison Organisation Network
DLT	Distributed Ledger Technology
ETL	ENISA Threat Landscape
GPS	Global Positioning System
ICS	Industrial Control Systems
ICT	Information and communications technology
IoT	Internet of things
IP	Intellectual Property
IT	Information Technology
ML	Machine Learning
OT	Operational Technology

[1] (ENISA, Glossary of Terms., 2018)

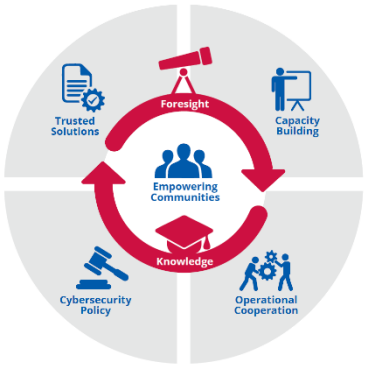
PESTLE	Political, Economic, Social, Technological, Legal and Environmental Dimensions (Analysis Method)
PTSD	Post-traumatic stress disorder
R&D	Research and Development
SFP	Science Fiction Prototype

2. INTRODUCTION

2.1 BACKGROUND

In line with the ENISA's European Union Agency for Cybersecurity'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 that included futurists, sociologists, business leaders, cybersecurity experts, and others, will now be used in practice to identify threats and challenges likely to emerge by 2030[4].

Drawing on the insights of previous ENISA projects and reports including "Looking into the Crystal Ball[5]" and "Foresight Challenges," the framework combines foresight methods with creative thinking approaches and co-creation/innovation methods; it leverages individual skills, knowledge, and reasoning in a collaborative setting. The overarching mission of this framework is to produce insight about the future and to enrich the dialogue between experts with various professions and backgrounds.

We believe that the key to defending the European Union is to prepare for the future; the future is made by us all and therefore to imagine it we need the input of a diverse range of people. Beyond identifying emerging futures, the agency will enable member states and other stakeholders to improve their cybersecurity based on the findings of the foresight exercise.

2.2 PURPOSE OF THIS EXERCISE

This study aims to identify and collect information on future cybersecurity threats that could affect the Union's infrastructure and services, and its ability to keep European society and citizens digitally secure. It is our intention to arm ENISA stakeholders with new insights with which to begin combatting future threats. The outcome generated by this practical application of

[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)
[5] (ENISA, Looking into the crystal ball., 2018)

the framework is the identification of 21 cybersecurity threats which may emerge or be exacerbated by the year 2030.

A secondary objective of this *Foresight on emerging and future cybersecurity threats 2030* exercise is to demonstrate that the foresight framework outlined in the *Foresight Challenges* report from 2021 can be applied in a practical context and to identify areas of opportunity in the framework to improve the applicability of ENISA's foresight activities.

Finally, the exercise of threat identification and prioritization serves an internal purpose of supporting each of ENISA's strategic objectives by providing relevant focus topic for future planning.

ENISA's strategy proposes concrete goals for the Agency in the form of seven strategic objectives that will set the priorities for European Union Agency for Cybersecurity in the coming years. The strategic objectives[6] 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

2.3 TARGET AUDIENCE

Our main target demographic for this project are stakeholders from the cybersecurity domain including national cybersecurity authorities, national and EU decision makers, experts, and practitioners. We specifically hope to target operational cybersecurity practitioners and response teams, using the identified threats and scenarios to build resilience and response arrays.

[6] (ENISA, A trusted and Cyber Secure Europe, 2020)

3. EMERGING CYBERSECURITY THREATS FOR 2030

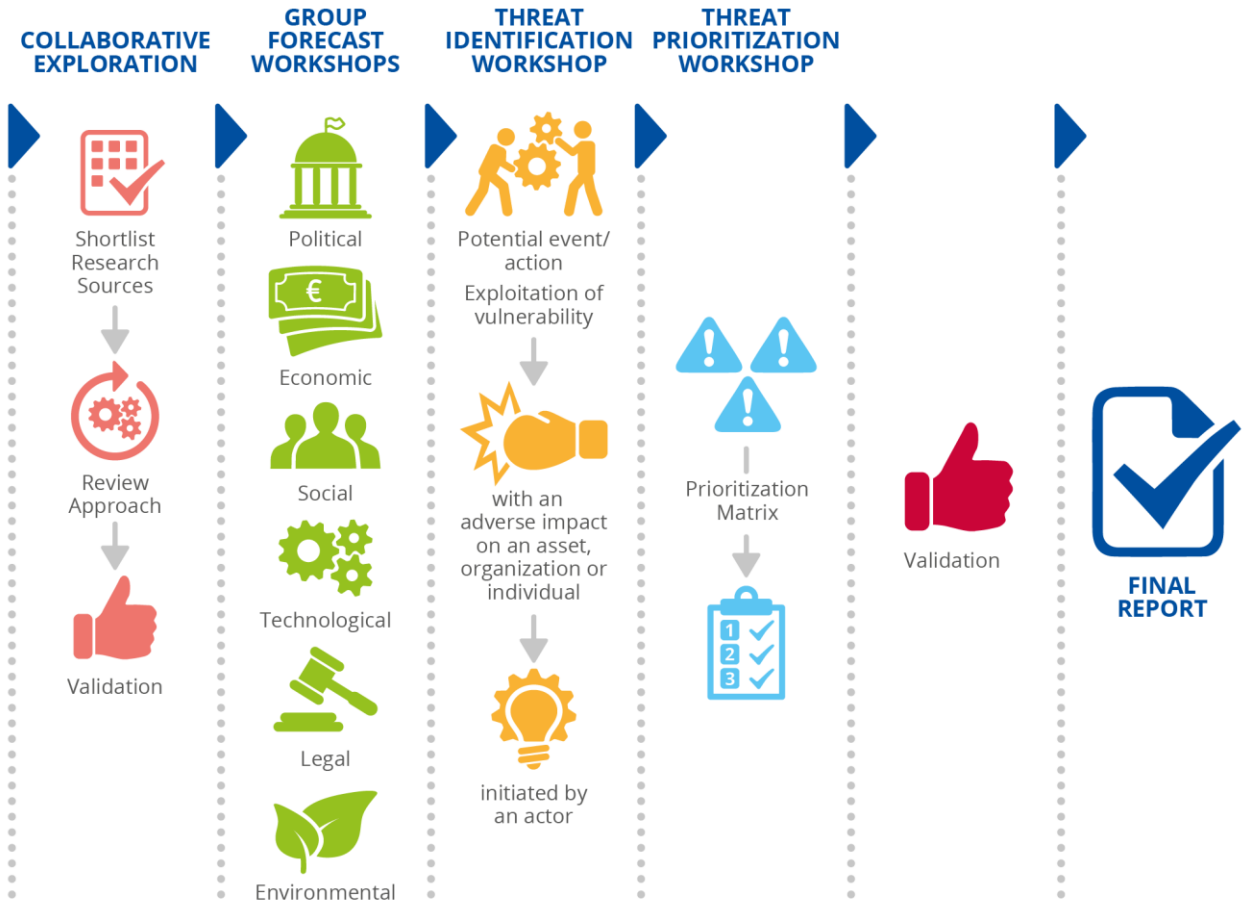
The threats identified and ranked within this report represent a range of topics, many of which are already relevant today. The outcomes of this exercise illustrate that in 8 years many of today's threats will remain pressing but will have shifted in character – increased dependencies and the democratization and development of new technologies add complexity to our understanding of threats. Our wish for readers of this report is that they are able to recognize shifts in the threat landscape and already begin preparations to ensure security and resilience in the face of morphing threats. In cybersecurity there is limited leeway to postpone actions that aid in the avoidance and mitigation of future risks; one must continuously anticipate approaching threats. These additional measures, however, need not come at the cost of necessary wide-reaching cybersecurity controls such as education, awareness, patching, etc.

Figure 2: Top 10 threats

Methodology

Through a series of workshops and interviews between March and August 2022, with relevant experts in the PESTLE (political, economic, social, technological, legal, and environmental) fields, ENISA has identified and ranked 21 threats that will increase in prevalence by 2030.

Figure 3: Foresight Exercise Methodology Overview



The methodology used has four phases. The first, "collaborative exploration," is a phase of trend research and information gathering that integrates expert knowledge, feedback, and validation. The second phase, "group forecast workshops," gathered groups of experts with experience in one of the PESTLE dimensions to further discuss, explore, assess, and prioritize the identified trends.

The third phase, "threat identification", is based on the threat casting[7] methodology for identifying emerging challenges within the next 10 years. To do so, small groups of cybersecurity experts are provided a scenario that combines prioritized trends. The scenarios are an integral part of the work in order to immerse in the future trends, however their description specific as it may be, does not influence the exploration and identification of threats. The scenarios merely serve as a medium to convey the content related to threats. The group explores this scenario by building personas and writing a short imaginative science fiction essay. The experts then assume an adversarial perspective to explore potential threat actors and vulnerabilities in the described future. This change in perspective enables the group to establish adversary motivations and define the possible threats.

The threats identified by the expert participants were then given scores on likelihood, impact, novelty, and whether the threat has been previously published by ENISA. Novelty is considered in this project in order to prioritize lesser-known threats.

[7] (West, 2017)

Further details about the methodology used can be found in Annex A.

Threat Descriptions

Each threat is described below with a focus on the top 10 most highly ranked threats. The threat actors are four main groups described in ENISA's 2022 Threat Landscape Report - state-sponsored actors, cybercrime actors, hackers-for-hire, and hacktivists[8].

The described methods refer to ENISA's current threat taxonomy[9]. It divides threats into the following high-level categories: physical attack (deliberate), unintentional damage / loss of information or IT assets, disaster (natural), failures/malfunctions, outages, eavesdropping/interception/hijacking, nefarious activity/abuse, and legal. The focus of this report is primarily on intentional threats; unintentional threats are considered here as vulnerabilities that may be exploited by a threat actor.

Each threat is also linked[10] to one or more of the scenarios to indicate the origins of the threat. The threat description also includes a link to ENISA's strategic objectives (SO). This linkage supports the connection between identified threats and ENISA's ongoing and future initiatives. ENISA's sixth strategic objective, foresight on emerging and future cybersecurity challenges, is relevant for each of the threats but is not included in the threat description as all threats are the result of a foresight exercise.

Table 1: Scenario-Trend Relationship Diagram

	SCENARIOS				
TRENDS	**Scenario 1**	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**
	The increased usage of new technologies in remote maintenance	Diminishing availability of fresh water	The increasing difficulty for law enforcement to access data stored on (encrypted) networks and the use of collected data	Non-traditional work structures like freelancing are rising in popularity ("gig economy")	Increasing introduction of (technical) legislation in Europe
	The use of Distributed Ledger Technologies is growing	The increasing geopolitical influence of communication providers	There is an increasing number of devices that are not (or are unable to be) regularly patched	Increasing reliance on automation and connectivity of sustainable energy production	Satellite control infrastructure is increasingly critical
	Advancement of deep fake technology	The increased political power of non-state actors	Decision-making is increasingly based on automated analysis of data	There is increasing popularity of everything as a service (XaaS) demand and supply	AI-based systems are increasingly deployed with bias or issues that impact inclusivity, safety, ethics, privacy, trustworthiness, and explainability
	Collecting and analyzing data to assess user behavior is increasing, especially in the private sector	The increasing relevance of (cyber) security in elections	The public health issues arising from the mental health problems of victims of cybersecurity	Automation of agricultural skills and workforce	The rise of digital authoritarianism
	The increased and improved connectivity of illegal businesses	The rise of smart cities	The capacity to control data about oneself (individual, company, or state) is becoming more desirable and more technically difficult	Industrial switch from fossil fuels to hydrogen or electric (demand)	Mass extinction and loss of biodiversity continues

[8] (ENISA, Threat Landscape Report, 2022)
[9] (ENISA, Threat Taxonomy, 2016)
[10] Linking threats to scenarios took place by ENISA during the preparation for the threat identification workshops.

Table 2: Overview of connections between threats and ENISA strategic objectives

STRATEGIC OBJECTIVES / THREATS	EMPOWERNG COMMUNITIES	CYBERSERCURITY POLICY	OPERATIONAL COOPERATION	CAPACITY BUILDING	TRUSTED SOLUTIONS	FORESIGHT	KNOWLEDGE MANAGEMNT
Supply chain compromise of software dependencies		✓	✓		✓	✓	✓
Advanced disinformation campaigns		✓	✓	✓		✓	
Rise of digital surveillance authoritarianism / loss of privacy		✓			✓	✓	
Human error and exploited legacy systems within cyber-physical ecosystems			✓	✓		✓	
Targeted attacks enhanced by smart device data			✓	✓		✓	✓
Lack of analysis and control of space-based infrastructure and objects	✓	✓	✓	✓	✓	✓	✓
Rise of advanced hybrid threats	✓		✓	✓		✓	✓
Skill shortage	✓	✓	✓	✓		✓	
Cross border ICT service providers as a single point of failure		✓	✓		✓	✓	
AI Abuse		✓	✓		✓	✓	

3.1 SUPPLY CHAIN COMPROMISE OF SOFTWARE DEPENDENCIES - #1

By 2030, we will see more and more integration of components and services combined into new products. As the market demands quick product release cycles, component-based programming

will strongly increase[11], leading to the reuse of code and the use of open-source code libraries. While some of these components will be regularly scanned for vulnerabilities, the combination of software, hardware and component-based code will create unmonitored interactions and interfaces[12]. This will lead to novel and unforeseen vulnerabilities, creating more opportunities for malicious actors to compromise the supply chain from the supplier and customer side. Financial and political motivations of these threat actors can lead to exploitation of software vulnerabilities, attacks on the configuration of hardware and software, malware injections in code libraries, as well as phishing attacks. This would lead to global supply chain issues and can be used by threat actors for political disruptions, financial gains, or espionage.

Adversaries may manipulate these software dependencies and development tools by adding backdoors to the code components. The easiest method for attackers is the manipulation of open-source libraries. If focusing more on commercial applications, the attackers can gain initial access through several techniques, including drive-by compromises or social engineering attacks. By placing trojans, droppers or rootkits into the software components of the suppliers, they can later gain network access to their ultimate target which uses the hardware or software component in their organization. Physical tampering with hardware in their production facilities are also a possibility. This would require the attackers to have physical access (or at the very least physical proximity) to the hardware component production facility. The attackers would infiltrate the facilities legitimately by having an insider working at the facilities who would be in an ideal position to tamper with the hardware for the purpose of data or system compromise.

Once compromised (leaving no trace) a state actor will purchase the manipulated hardware or software, install it across the country, and open themselves up to a very widespread attack. Another case can be the compromise of a widely used private company with access to sensitive data, as seen in the SolarWinds incident[13].

<table>
<tr><th colspan="4">Threat #1 - Score 25</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored groups, criminal organizations</td><td>Relevant Scenario(s)</td><td>Scenario 2, 4</td></tr>
<tr><td>Probable Methods</td><td>Sabotage, Theft, Network Reconnaissance, Malicious code, Abuse of Information Leakage</td><td>Topics for future SPD</td><td>Transparency in critical infrastructure supply chain (2nd and 3rd level), CE Certification schemes, CVD, Awareness raising and education, software bill of materials / Chain of trust</td></tr>
<tr><td>Probable Impacts</td><td>Disruption, Malfunction, Data Loss, Data Leakage</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO2, SO3, SO5, SO7

Supply chain compromises are very relevant for EU policies that cross nations and sectors (SO2). The sheer scale of supply chain attacks also demands effective operational cooperation in the event of an incident (SO3). These threats are in direct opposition to ENISA’s SO5 – high level of trust in secure digital solutions. Finally, comprehensive knowledge management and education on potential supply chain attacks is necessary to mitigate the threat (SO7).</td></tr>
<tr><td colspan="2">Example: State-sponsored actors insert a backdoor in a well-known and popular open-source library on online code repository. They use this to infiltrate information from most major European corporations and use the information to blackmail leaders, espionage, or otherwise initiate disruptions across the EU.</td></tr>
</table>

[11] (ENISA, Understanding the increase in Supply Chain Security Attacks, 2021)
[12] (Jubb, 2022)
[13] (Newman, 2021)

3.2 ADVANCED DISINFORMATION / INFLUENCE OPERATIONS (IO) CAMPAIGNS - #2

In 2030, non-state actors like criminal groups, hackers-for-hire as well as government actors will likely have the technological capabilities (e.g., deepfakes) to expand their disinformation efforts in the EU to manipulate communities. While the application of deepfake technology allows for illicit financial enrichment of criminal groups or individuals, the primary motivation for disinformation campaigns through faked identities is (geo)political and will likely be predominantly performed by state actors and other politically motivated actors.

Data sources are now immeasurable; adversaries can train their AI for deepfake attacks[14] with a wide range of publicly available videos, pictures, and voice recordings of individuals (even those not in the public sphere). Biometric facial images are particularly vulnerable to morphing attacks in which the threat actor can, to a high degree of accuracy, impersonate their target. Deepfake technology can also create unreal faces that the human eye is unable to differentiate from real faces. Therefore, adversaries can create realistic avatars that go beyond the current social media[15] bots that already have elaborate profiles. The bots of the future that can influence elections and public trust also share videos of themselves on social media to participate visibly in the debate. Disinformation campaigns could be further reinforced with AI text or voice analysis to provide personalized responses to individuals.

<table>
<tr><th colspan="4">Threat #2 - Score 20</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored groups, criminal organizations, hackitvists</td><td>Relevant Scenario(s)</td><td>Scenario 1, 2, 5</td></tr>
<tr><td>Probable Methods</td><td>Fraud, Unauthorized access, Session Hijacking, Identity Theft, Abuse of Personal Data</td><td>Topics for future SPD</td><td>Advanced awareness activities, deepfake identification research, authentication best practices</td></tr>
<tr><td>Probable Impacts</td><td>Distrust, disinformation, financial damage</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO2, SO3, SO4

EU policies need to be prepared to address disinformation (especially when powered by deepfakes and digital IDs) (SO2). Because these attacks will be difficult to detect, it is paramount that cross-border mitigations and incident response be enabled (SO3). These attacks will test the capabilities of EU Member States – from non-experts to highly-skilled professionals (SO4).</td></tr>
<tr><td colspan="2">Example: A state-sponsored actor may impersonate a political rival by using deepfakes and spoofing the candidate’s digital identity, significantly impacting election results.</td></tr>
</table>

3.3 RISE OF DIGITAL SURVEILLANCE AUTHORITARIANISM / LOSS OF PRIVACY - #3

Criminals are increasingly being identified through technologies like location tracking, public cameras, and facial recognition[16]. In the future, this may encourage states, and likewise private actors, to vastly expand the use of these technologies. Through technologies like facial recognition in the public sphere, increased digital surveillance on internet platforms, or the adoption of digital identities, European individual freedoms may be curtailed for the sake of safety and security. Access to this data will enable and encourage law enforcement agencies and other government entities to track potential suspects. These data stores may also become a huge target for criminal groups who are able to sell data online for individuals based on just a photo. The private sector also plays an important role – especially when major facial recognition technologies or content platforms are dominated by a single market leader. Single providers

[14] (Shein, 2022)
[15] (ENISA, Threat Landscape, 2021)
[16] (ENISA, Personal Data Breaches, 2020)

who provide facial recognition technology or content platforms will be targeted for the troves of consolidated voice and image data available. Furthermore, the actions of private corporations may not always align with data protection and security requirements.

Governments (including law enforcement) and private enterprises as part of public-private partnerships can, within their legal boundaries, legitimately collect personal data - including biometric data. This creates challenges[17] for privacy regulators and the public to make sure the laws that protect their privacy are enforced. Additionally, it requires all entities collecting this data to have the necessary defence mechanisms in place. Once adversaries gain access to the network, they can engage in automated collection of data, potentially including a command and scripting interpreter as well as APIs, command line interfaces, or extract, transform, and load (ETL) services in cloud environments. One use case would include an abuse of the collected data by law enforcement or online vigilante communities to track down potential criminals.

<table>
<tr><th colspan="4">Threat #3 - Score 18</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored groups, criminal organizations</td><td>Relevant Scenario(s)</td><td>Scenario 3, 5</td></tr>
<tr><td>Probable Methods</td><td>Man in the middle, Malicious Software, Use of Rogue Certificates, Abuse of personal data</td><td>Topics for future SPD</td><td>Holistic topic, more detailed analysis on risks and layers needed (jurisdiction, privacy, EU – national legislation). Analysis via guidelines and foresight exercise</td></tr>
<tr><td>Probable Impacts</td><td>Privacy breaches, human rights abuses</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO2, SO5

Mitigating this threat requires strong cybersecurity and data protection policies (SO2) and a high level of trust in solutions (e.g. digital IDs) (SO5).</td></tr>
<tr><td colspan="2">Example: An authoritarian leader uses their power to retrieve databases of information about individuals who have visited their country – from both public and private entities. They track all those who participated in anti-government protests, put them on a watch list, and subsequently are able to manipulate those individuals' access to national services like voting, visits to their healthcare providers, or access to other online services.</td></tr>
</table>

3.4 HUMAN ERROR AND EXPLOITED LEGACY SYSTEMS WITHIN CYBER-PHYSICAL ECOSYSTEMS - #4

In 2030, IoT permeates large parts of transport, power and water grids, and industrial infrastructure to increase efficiency and improve intelligent decision-making. Furthermore, we will see a significant increase in the number of smart devices the average user has associated to them (as of 2021, the average person had seven smart devices).[18] Because of this, it may become exceedingly difficult to maintain and manage all devices, especially from a security perspective. Additionally, the manufacturers of the smart devices will likely be unsuccessful on educating end-users of the need for device maintenance. The fast adoption of IoT and the ongoing skill shortage will lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem by 2030, leading to IT and OT security maintenance issues arising from the misconfiguration, delayed maintenance, and inadequate end-of-life support of discontinued IoT software. In addition to these issues, threat actors may deploy intelligent attacks using techniques such as Generative Adversarial Networks (GAN), which may dramatically reduce the detection rate of cyberattacks. One example of the use of GAN would be to target servers distributing patches in order to disrupt scheduled updates[19]. Because of the criticality of the

[17] (ENISA, Foresight Challenges, 2021)
[18] (BSI-Magazin, 2021)
[19] (Shi, 2021)

devices, this can create a systemic risk, leading to outages, damage as well as the interception of data between the devices.

On the end user side, IoT devices are often managed by mobile devices running on iOS or Android. The end-users communicate through their mobile applications with the smart devices that are part of their home, transport or other surrounding. Adversaries can try to get initial access to the mobile devices by biometric spoofing, brute force attacks, or exploiting vulnerabilities on the device. Once they have access to the phone and the legitimate communication channels between the end-user phone and the infrastructure, they can tamper with the smart devices, laterally move to the network or get access to the account that manages the smart devices.[20] In an industrial ecosystem, adversaries could get initial access through employees by social engineering attack or through their endpoints, move laterally within the corporate network and look for internet accessible devices that are connected to the industrial control systems. Additionally, attacks could succeed through transient cyber assets that are deployed with an insecure configuration – including those from third party suppliers and partners.

<table>
<tr><th colspan="4">Threat #4 - Score 18</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored groups, cyber criminals, hacktivists</td><td>Relevant Scenario(s)</td><td>Scenario 1, 3, 4</td></tr>
<tr><td>Probable Methods</td><td>Tampering, Failure of Communication links, Denial of Service, Malicious activity, Manipulation of Information, Targeted Attacks, Brute force, Unauthorized Physical Access</td><td>Topics for future SPD</td><td>Guidelines for securing the IOT[21], Certification Schemes, Secure communication standards, guidelines for secure storage of data, * Processes related to security-by-design, Software bill of materials / Chain of trust, Economical value of cyber-attacks and cyber security</td></tr>
<tr><td>Probable Impacts</td><td>Malfunction, Failures and Outages, Physical Damage</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO3, SO4

Incidents involving legacy equipment typically impact cross-border critical infrastructure (SO3.) More expertise and experience in securing a range of products and retrofitting legacy systems requires additional education and research into these fields (SO4).</td></tr>
<tr><td colspan="2">Example: Manuals for all legacy OT equipment are available online and studied primarily by state-sponsored groups. Once a vulnerability is found, they target user devices or other IoT products used at the plant. Cyber criminals begin a new form of ransomware in which they bring down important infrastructure and demand payment – given that the operator likely lacks the resources to solve the issue themselves.</td></tr>
</table>

3.5 TARGETED ATTACKS (E.G. RANSOMWARE) ENHANCED BY SMART DEVICE DATA - #5

In 2030, the collection of behavioural data will have exponentially increased. The use of smart devices in our daily lives will significantly increased; data from all aspects of life will be collected, leading to an accurate and unique behavioural profile of each user. Collected data may include (among other sources) health data in from wearables and medical equipment, or IoT devices in Smart Homes that collect information of behaviour at home, movement data, or behaviour across online platforms. As the smart devices will often be insecure due to the unwieldy

[20] (SOCRadar, 2022)
[21] (ENISA, Guidelines for Securing IOT, 2020)

amounts of devices and lack of end user awareness, this data is at danger of being exploited[22]. Intelligent edge devices are already difficult to protect from manipulation and eavesdropping. Criminal groups will try to get access to troves of data to tailor social engineering attacks based on the behaviour profile of the user. The level of sophistication of these social engineering attacks will challenge end users, law enforcement and governments alike to find new ways to prevent social engineering and improve authentication.

Attackers may obtain initial access through internet-connected smart devices that are unpatched, or still running default settings. Criminals and hackers-for-hire[23] will gather victim identity information, credentials, and contact information to gain initial access and then move laterally within the network to access more sensitive information. The attackers will use automated data collection and infiltration, correlate and interpret the data to create the behavioural profile of their victim. Adversaries will use persistence techniques to maintain their foothold. With the behavioural profile, they will try to get access to financial assets, use the profile to spoof high-profile individuals within the victim's network or sell the collected data on the black market.

<table>
<tr><th colspan="4">Threat #5 - Score 18</th></tr>
<tr><td>Probable Threat Actors</td><td>Cybercrime actors, hackers-for-hire</td><td>Relevant Scenario(s)</td><td>Scenario 1, 3, 4</td></tr>
<tr><td>Probable Methods</td><td>Denial of Service, Interception of Information, Social Engineering, Unauthorized activities, Data breach</td><td>Topics for future SPD</td><td>OES education activity, backup and recovery plan, general security guidelines, Economical value of cyber-attacks and cybersecurity, Awareness raising and education, Software update lifecycle, Software bill of materials / Chain of trust</td></tr>
<tr><td>Probable Impacts</td><td>Financial Damage, Privacy Breaches</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO3, SO4, SO7

Targeted attacks will be more quickly resolved with the operational support of EU-wide response teams (SO3) and cutting-edge capabilities (SO4) and knowledge (SO7).</td></tr>
<tr><td colspan="2">Example: Cybercriminals may use the increased amount of available data from smart devices and analyze it with AI to create behavioral models of their victims for spear phishing campaigns or stalking.</td></tr>
</table>

3.6 LACK OF ANALYSIS AND CONTROL OF SPACE-BASED INFRASTRUCTURE AND OBJECTS - #6

The early 2010s and 2020s have started a new era of space travel, with private companies joining governments in the pursuit to explore our universe. By 2030, the space sector will likely transform even more with more investments of private actors, partnerships between private companies and governments, and increased geopolitical and commercial competition in space. The fast growth of this sector will enable many key services. Despite the advances made in recent years, the sector is still emerging as a focus topic for the security community.

From a security perspective, there is a lack of understanding, analysis and control of space-based infrastructure. Without a broader EU-wide focus, building up a strong defence of space infrastructure may be too slow (e.g. R&D projects that take time to be planned and budgeted for.) This also means that there may be a lack of timely preparation for the identification and

[22] (ENISA, Threat Landscape, 2021)
[23] (ENISA, Threat Landscape Report, 2022)

exploitation of unknown vulnerabilities[24] (zero-days) – if the resources are not appropriately allocated. Markets incentivise private companies to execute and innovate faster, and to lower cost at the expense of cybersecurity. Private companies may try to use this to sabotage their rivals; governments may try to exploit vulnerabilities to create a competitive geopolitical advantage in space; and criminal groups will use the vulnerabilities to extort companies for financial gains and to create havoc.

Because of the intersections between private and public infrastructure in space, attackers can gain initial access to space-based infrastructure by either targeting the private actors, government agencies or the individuals interacting with the infrastructure. As governments and societies largely depend on satellites (e.g. GPS), state-sponsored attackers and Hackers-for-Hire will try to get initial access to hardware through supply-chain attacks and use techniques to maintain their presence within the space infrastructure – including base stations. [25]Base stations are transceivers that connect satellites to a central terrestrial hub that connects the satellite to a network. They are a key element that attackers will target with denial-of-service attacks to disrupt critical military and civilian systems. Attackers will use available techniques to evade defence and detection mechanisms but remain dormant until they execute their exploit strategically, e.g. during a conflict as a mean for hybrid-warfare. The introduction of space-based weapons may shift the geopolitical paradigm.

<table>
<tr><th colspan="4">Threat #6 - Score 18</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored actors, Cybercrime actors, Hackers-for-hire</td><td>Relevant Scenario(s)</td><td>Scenario 5</td></tr>
<tr><td>Probable Methods</td><td>Unauthorized use of IPR Protected Resources, Targeted Attacks, Fraud, Sabotage, Information Leakage, Session Hijacking, Malicious Software</td><td>Topics for future SPD</td><td>Certification schemes, frequent risk assessment plans, international cooperation, threat landscape for space</td></tr>
<tr><td>Probable Impacts</td><td>Damage, Outages, Malfunctions</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO1, SO2, SO3, SO4, SO5, SO7

This threat will be reduced through a multi-stakeholder approach that includes policymakers, incident response teams, R&D teams, certification programs, and knowledge management.</td></tr>
<tr><td colspan="2">Example: State-sponsored attackers access space infrastructure, build up their capabilities and knowledge of the technology, and secure their presence to execute attacks. Their aim may be to create infrastructure malfunctions as a statecraft tool to sabotage other governments during geopolitical conflicts.</td></tr>
</table>

3.7 RISE OF ADVANCED HYBRID THREATS - #7

By 2030, cyberattacks will become more sophisticated and will be matched with physical or offline attacks. Attack methods are constantly evolving and are often combined – in sequence and in parallel – to reach their goals. These hybrid operations are more difficult to detect and defend against due to their complexity and the tendency to treat each attack individually. With a new modus operandi, detection tools need greater correlation capabilities including connecting seemingly unrelated events. They therefore pose a growing challenge for governments, companies, and citizens alike. In the past, hybrid attacks were primarily executed by state actors as a combination of traditional and cyber warfare. In 2030, hybrid threats have evolved to

[24] (Erwin, 2022) (Forum, 2022)
[25] (Tim Starks, 2022)

apply new technologies and combine different types of exploit mechanisms in order to evade existing response systems.

For example, attackers will also increasingly use artificial intelligence and deep learning to combine their capabilities[26] to create new, unforeseen modus operandi. Attackers will use a simultaneous combination of techniques to gain initial access, including the collection of big data to tailor their spear phishing campaigns, machine learning to interpret the data, develop new tools to evade defence mechanisms and combine the physical and the virtual to execute their attacks. With the increase of smart devices, cloud usage, more online identities and social platforms, as well as digital IDs issued by governments, attackers will have a variety of new realms to use and combine to create creative attack vectors.

<table>
<tr><th colspan="4">Threat #7 - Score 14</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored actors, hackers-for-hire, cyber criminals</td><td>Relevant Scenario(s)</td><td>Scenario 2</td></tr>
<tr><td>Probable Methods</td><td>Unauthorized Access, Social Engineering, Abuse of personal data, Remote Command Execution, Malicious Activity</td><td>Topics for future SPD</td><td>AI security best practices, end-user awareness campaigns, secure data processing standards, common hybrid threat combinations, guidelines on developing trustworthy technology</td></tr>
<tr><td>Probable Impacts</td><td>Privacy breaches, outages, failures/malfunctions</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO1, SO3, SO4, SO7
Combatting hybrid threats can be achieved through activation of a variety of cybersecurity communities (SO1), including incident response entities (SO3). This increase in hybrid attacks with new technologies requires cutting-edge capabilities (SO4) and knowledge (SO7.)</td></tr>
<tr><td colspan="2">Example: Hackers are hired by a corporation to investigate the new technology being developed by a competitor. In their quest, they are able to retrieve metadata, view code, and set up a machine learning algorithm that continuously collect changes to the code and then continuously accesses user account to prevent monitoring systems from recognizing that the attacker is in the network. In parallel they obfuscate the activity by spreading fake news about insider trading and industrial espionage from a third competitor by dropping fake evidence of physical intrusion.</td></tr>
</table>

3.8 SKILL SHORTAGES #8

In 2022, the skill shortage[27] contributes to most security breaches, severely impacting businesses, governments, and citizens. By 2030, the skill shortage problem will not have been solved. While the growth of unfilled cybersecurity jobs has levelled off, the skill shortage[28] will continue to pose a significant risk to society and governments. One relevant factor that will impact the threat in 2030 is organizational willingness (and resources) to expand staff and develop talents. The implementation of cybersecurity features will also suffer due to lack of skills and overall maturity of cybersecurity features, even if the willingness is there.

As technology integrates more and more into our lives, average citizens may become apathetic - all their communications and actions are managed somewhere else, over which they have no

[26] (Shein, 2022)
[27] (Fortinet, 2022)
[28] (Hurst, 2022)

control. This risk will be compounded by the interaction between new technologies and legacy technology for which the workforce has not been trained – knowledge of legacy technologies is not being passed on quickly enough to manage the risk in 2030. On top of the legacy skill shortage, new technologies like smart devices, artificial intelligence, space-based infrastructure or quantum computing will pose new cybersecurity challenges. Criminal groups will target organizations, institutions, and companies that have a large amount of unfilled cybersecurity jobs to find vulnerabilities and exploit these vulnerabilities for financial gain.

Threat actors will analyse organizational skillsets and deficiencies to gain insight into weaknesses in defence, potential vulnerabilities, and opportunities to exploit their systems and networks. Public job advertisements often give detailed information as to which skillsets are currently lacking within a company or a government agency, giving the attackers insights into possible entry vectors. In addition, attackers will try to gain open- and closed-source information to gather organizational and network information to spot legacy systems with known vulnerabilities. For example, a job posting from a local power plant may share the vendor and product type for which they need support- this provides threat actors with ample time to investigate product-specific vulnerabilities. Also, in the development of new technologies, the employees qualified to implement security do not have enough bandwidth to apply security before go-to-market due to lack of overall skilled workers.

<table>
<tr><th colspan="4">Threat #9- Score 14</th></tr>
<tr><td>Probable Threat Actors</td><td>Cybercrime actors, Hackers-for-hire, state-sponsored actors</td><td>Relevant Scenario(s)</td><td>Scenario 3, 4</td></tr>
<tr><td>Probable Methods</td><td>Spear Phishing Attacks, Social Engineering</td><td>Topics for future SPD</td><td>extend ECSM into a whole year, policy recommendations for Commission to adapt to digital society, EU cybersecurity education programs,</td></tr>
<tr><td>Probable Impacts</td><td>Financial Damage, Outages</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO1, SO2, SO3, SO4

Cybersecurity communities need to come together to combat the skill shortage (SO1.) This includes with regard to policies (SO2), incident response (SO3), and tangible capabilities and competencies (SO4).</td></tr>
<tr><td colspan="2">Example: The skill shortage leads to an increase of online job advertisements that tell attackers the technologies that each organization is using and the approximate number of empty positions. A state-sponsored actor may use this to their advantage as a part of a larger campaign to tamper with critical infrastructure in another country.</td></tr>
</table>

3.9 CROSS-BORDER ICT SERVICE PROVIDERS AS A SINGLE POINT OF FAILURE #9

In 2030, technological interconnectedness will be strengthened. The physical-cyber border will be further blurred as infrastructure sectors such as transport, healthcare, electric grids and industry[29] are increasingly reliant on ICT service providers to connect to the internet and to manage all inter-device communications. Even though their responsibility for upholding a functioning society was significant back in 2022, their importance grows even more by 2030. ICT service providers and their infrastructure – including satellite technology – are the backbone of society and therefore may be a single point of failure. Smart cities are an example of how even more critical operational networks will be in 10 years. Hence, these service providers will likely be targeted by governments, terrorists and criminal groups. Exploiting vulnerabilities in

[29] (ENISA, Threat Landscape, 2021)

their infrastructure, using hybrid attacks to get access to their networks, endpoints, data centres or other physical components of the ICT infrastructure could cripple cities and whole regions. Foreign governments may try to use this to destabilize nations, terrorists to fuel fears and achieve political goals, and criminal groups to hold cities hostage.

ICT infrastructure[30] is likely to be weaponized during a future conflict. ICT providers will have to defend against state-sponsored, persistent and highly developed attacks that draw on insights from governmental intelligence agencies and offensive cyber capabilities. The resources that would be dedicated to such an attack are significant – attackers would take time to evade traditional response functions and will likely deploy hybrid attacks for initial access and newly developed exploits with command-and-control capabilities. Because the ICT sector connects so many critical services, it will be targeted by techniques like backdoors, physical manipulation, and denials of service due to the scale of damages that can be achieved.

<table>
<tr><th colspan="4">Threat #10 - Score 13</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored actors, Hackers-for-hire</td><td>Relevant Scenario(s)</td><td>Scenario 2</td></tr>
<tr><td>Probable Methods</td><td>Fraud, Theft, Corruption, Terrorist Attack, Network Traffic Manipulation, Manipulation of Hardware or Software, Abuse of Authorizations</td><td>Topics for future SPD</td><td>How to best implement oversight for non-EU entities, How to enforce what is proposed – importance of EU market (example GDPR), Economical value of cyber-attacks and cyber security, Transparency in critical infrastructure supply chain (2nd and 3rd level)</td></tr>
<tr><td>Probable Impacts</td><td>Outages, Damage/Loss, Unavailable Critical Infrastructure</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO2, SO3, SO5

While cybersecurity policies help to prevent cross-sector incidents (SO2), operational support will be necessary in the event of an incident (SO3). Trust in critical infrastructure providers is essential (SO5).</td></tr>
<tr><td colspan="2">Example: A state-sponsored actor aims to temporarily cripple a region during an active conflict by installing malware that disrupts all critical functions of the ICT provider. Without operational cities, roadways, and communication channels, the region is essentially crippled without the ability for civilians to go about their daily lives and the responsible parties limited in their ability to maintain defense monitoring systems and to collaborate to develop response options and methods for bringing the necessary systems back online.</td></tr>
</table>

3.10 ABUSE OF AI - #10

AI can be manipulated from its inception and throughout its lifecycle through training manipulation and adversarial attacks[31] (among others). Unconscious bias in AI is a well-known concern in the early 20s, however in 2030 there is a real threat of intentional manipulating AI algorithms and training data. Likewise, any corrupted training of AI algorithms may train them to make incorrect decisions with respect to the high-risk sectors (defined by the European Commission[32]).

[30] (Allianz, 2016)
[31] (West, 2017)
[32] (Commission, 2022)

Threat actors will try to leverage the power of AI applications to shape the decision-making outcomes and to gather information on potential victims. For example, they may tamper with training data sets to create dysfunctional and harmful AI applications – this may include crowd sourced data projects. AI can be used to sift through the mass amounts of data about individuals to correlate data points about them - the presence of this capability may lead to an increase in stalkerware. Further, attackers may use AI for offensive or criminal purposes – such as analysing user behaviour to create highly developed spear phishing or hybrid campaigns.

AI can be used to enhance many nefarious activities such as: creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots, data poisoning, etc.

<table>
<tr><th colspan="4">Threat #10 - Score 12</th></tr>
<tr><td>Probable Threat Actors</td><td>State-sponsored actors, cyber criminals, hackers-for-hire</td><td>Relevant Scenario(s)</td><td>Scenario 1, 3, 5</td></tr>
<tr><td>Probable Methods</td><td>Spoofing, Denial of Service, Malicious code, Unauthorized Access, Targeted Attacks, Misuse of Information, Man in the Middle Attack</td><td>Topics for future SPD</td><td>AI security best practices, guidelines for secure software, AI regulation, certification schemes, Detection of training data manipulation</td></tr>
<tr><td>Probable Impacts</td><td>Biased decision-making, privacy violations</td><td colspan="2" rowspan="2">Relevant strategic objectives: SO2, SO3, SO5

The inclusion of AI topics in cybersecurity policies (SO2), rapid operational support (SO3), and trusted certification schemas (SO5) will help to reduce the risk of AI-related threats.</td></tr>
<tr><td colspan="2">Example: A state-sponsored actor wants to sow discord in a population before an election and manipulates the learning data of a law enforcement algorithm to target specific populations, causing widespread protests and violence. They are also able to deduct information about the political opponents themselves by using an AI analysis of the individuals' whereabouts, health history, and voting history – the correlation of such personal data will likely only be feasible with the use of AI tools.</td></tr>
</table>

3.11 ADDITIONAL THREATS

The following threats were included on the final prioritized threat list but based on the ranking system were not in the top 10.

Table 3: 2030 Top threats continued

#	Threat Name	Threat Description
11	Increased digital currency-enabled cybercrime	By 2030, digital currency-enabled cybercrime will increase rapidly. Cryptocurrencies, and the broad market adoption of them, already have enabled organized crime to expand their reach. Because digital currencies will be very commonly used as an investment asset and means of payment in European markets, organized crime may be able to expand their targets. This means that cybercrime groups offering professional services (cyber-attacks) will be better funded because of an increase in the efficiency and effectiveness of their efforts.

12	Exploitation of e-health (and genetic) data	The amount of genetic and health data increases tremendously by 2030 and is in the hands of many stakeholders in the public and private sectors. Vulnerabilities in e-health devices and databases containing very sensitive and/or genetic information may be exploited or used by criminals to target individuals or by governments to control populations, e.g., using diseases and genetic diversity as a reason for discriminating against individuals. Genetic data may further be abused to aid law enforcement activities like predictive policing or to support a more regimented social credit system.
13	Tampering with deepfake verification software supply chain	By 2030, deepfake technology will be widely used. It may be used as a form of harassment, evidence tampering, and provoking social unrest. Although there will likely be a rapid influx of verification software that analyses videos and voice to verify the identity of individuals[33], the urgent market demand leads to programmers cutting corners. This software will be highly targeted by anyone wishing to use deepfakes for illegal or unethical purposes.
14	Attacks using quantum computing	In 2030 quantum computing resources will be made more widely available, allowing threat actors to use quantum computing to attack existing deployments of public key cryptography. Likewise, there is a risk that threat actors collect sensitive encrypted data now, aiming to decrypt it once quantum computing is accessible. This is especially relevant for current digital IDs that use asymmetric cryptography to authenticate.[34]
15	Exploitation of unpatched[35] and out-of-date systems within the overwhelmed cross-sector tech ecosystem	Everything-as-a-service leads to a multitude of tools and services that require frequent updates and maintenance by both consumers and providers. This combined with the skill shortage presents a difficult to manage surface of vulnerabilities that can be exploited by threat actors. Furthermore, the complexity of the supply chain fosters confusion on where responsibilities for security lie. For governments, this creates more backdoors for espionage while cyber-criminals can exploit the unpatched and outdated services for financial gains. This is especially true when critical infrastructure is in the hands of the private sector or when national security data is reliant on singular private entities.
16	AI disrupting/enhancing cyber attacks	Escalation as a result of AI-based tools. Attackers will use AI-based technologies to launch attacks. In order to defend against those attacks and even to launch counter measures, there must also be defensive AI-based weapons. Behaviour of the AI in these cases is difficult to test, measure and control – if speed of response is valued.
17	Malware insertion to disrupt food production supply chain	Due to increased automatization and digitalization of food production, food supply chains[36] can be disrupted by a range of threat actors with medium-high resources. Denial of service attacks on packaging plants, for example, can prevent continued food operations; processed food manufacturing tools may be manipulated to change the compounds in the food itself. Attacks like these can lead to a food shortage, economic disruptions, and in the worst case, poisoning.

[33] (ENISA, Personal Data Breaches, 2020)
[34] (Smart, 2021)
[35] (Micro, 2019)
[36] (ENISA, Understanding the increase in Supply Chain Security Attacks, 2021)

18	Technological incompatibility of blockchain technologies	Until 2030, several regionally based blockchain technologies are created by different groups of governments to create an international "gold standard". This is driven by a societal lack of trust in blockchain that has accumulated over the last years. Each technology group aims to gain a competitive advantage. This gives rise to a period of technological incompatibility of blockchain technology which leads to failures, malfunctions, data loss and the exploitation of vulnerabilities at the interfaces of the different blockchains. This creates challenges for ecosystem management and data protection, furthers distrust, and negatively affects trade and GDP growth.
19	Disruptions in public blockchains	Blockchain has been implemented in nearly all aspects of society in 2030[37]. Unfortunately, security expertise in the area of blockchain did not advance significantly, creating a slew of vulnerabilities that may be exploited in the future. Locally unavailable blockchain technology will, for example, prevent access to voting, legal transactions, and even security systems. Another possible attack vector is exploited by partitioning the bitcoin network by hijacking IP address prefixes. This can cause, for example, duplicated spending and thus economic damage.
20	Physical impact of natural/environmental disruptions on critical digital infrastructure	The increased severity and frequency of environmental disasters causes several regional outages. Redundant back-up sites that maintain the availability of critical infrastructure will also be affected.
21	Manipulation of systems necessary for emergency response	Manipulation of sensors with connections to emergency services may overload services like ambulances, police, firefighters, etc. For example, call centres may be overloaded with inauthentic calls or fire alarms may be manipulated to injure specific individuals or to obscure emergency response teams' ability to locate the issue. Similarly, mass panics that overload emergency systems may also be provoked through the use of social media.

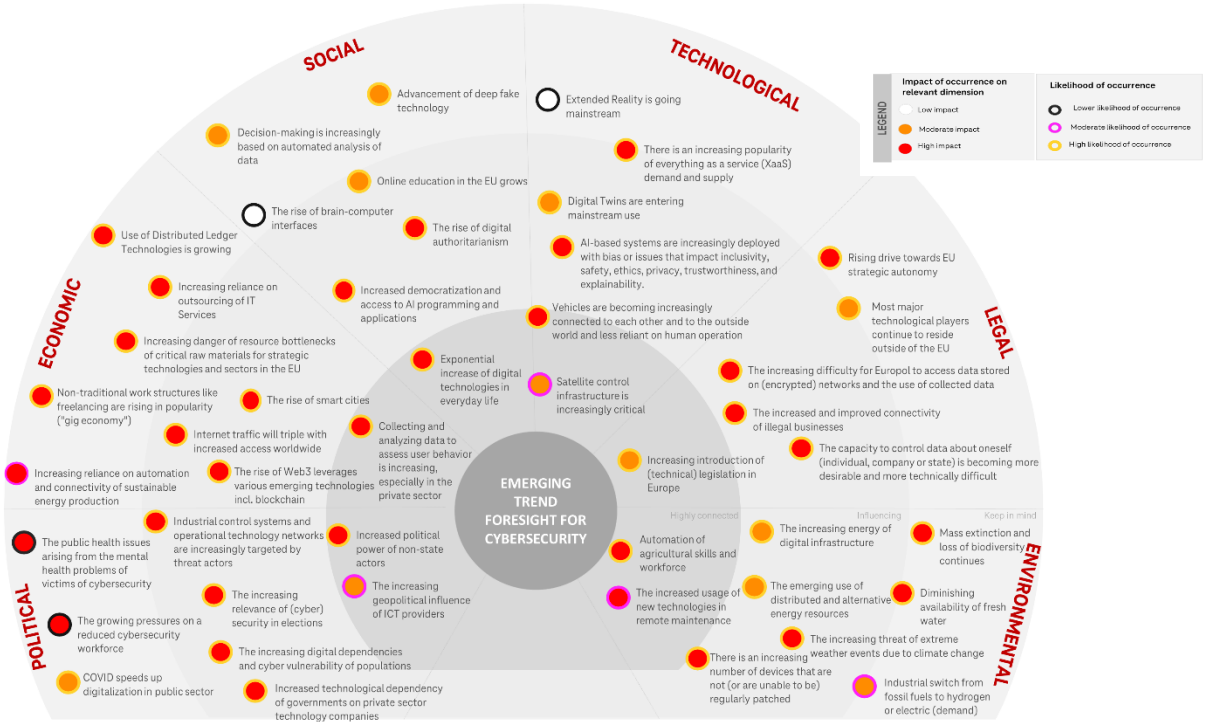
[37] (ENISA, Threat Landscape, 2021)

4. 2030 TRENDS

To identify the threats, the project team initiated an in-depth research project on future trends as a first step. Based on this research, the team created a long list of trends that was then narrowed down, discussed and analysed in individual PESTLE-themed (**p**olitical, **e**conomic, **s**ocial, **t**echnological, **e**nvironmental, and **l**egal) workshops by a diverse expert group[38]. As following step, the threats named in the previous chapter were identified by cybersecurity experts based on an examination of possible futures as derived from current and possible future trends (in the form of science fiction prototypes and scenarios).

Below is an overview of the prioritized trends, color-coded based on their scores on impact and likelihood (on a scale of 1-5). To simplify the image, the trends are rated based on a combination (impact x likelihood) of the experts' evaluations and have been assigned a prioritization of "high, moderate or low". The further inward the trends are positioned, the more interconnected they are. For additional information on the connection between trends see figure 5.

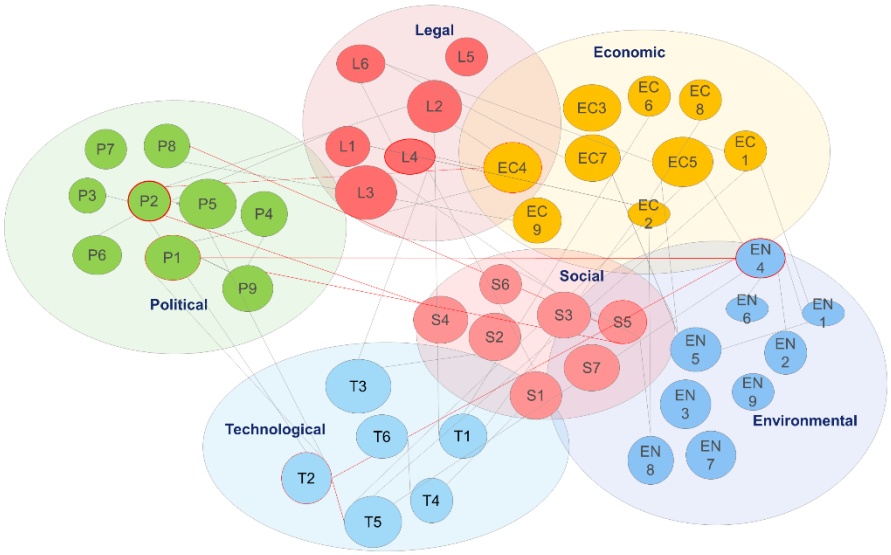
Figure 4: PESTLE Trend Radar



Foresight is a multifaceted tool through which targeted collective wisdom can be collected and through which a lot of insightful secondary data can be extracted. As participants evaluated potential trends, the conversations also shifted towards relationships between the trends. These references and relationships are visualized in the following graphic.

[38] (West, 2017)

Figure 5: Interaction between trends



This image shows the connections that the experts made between the different trends during the workshops. The trend names within the PESTLE[39] dimensions have been translated into trend IDs to simplify the image. The trend IDs shown in Figure 5 (above) can be found in the section below.

In some cases, the relationship of one trend to other trends led to clustering, so new trend labels were formulated to cover all the trends within them. In other cases, the trends were considered separately and commonalities between the trends were identified. These similarities are illustrated in this visualization by the gray connecting lines. Particularly salient links between trends are connected by a red line. As described earlier, participants rated the trends according to their potential impact and the likelihood of their occurrence - those that were rated particularly highly are outlined in red.

4.1 PRIORITIZED TRENDS

This section documents the key trends from each PESTLE dimension. The trends listed below were the trends that received the highest likelihood and greatest impact ratings during the workshops. Note that each trend may fall into more than one category, but it is listed based on the expert working group that ranked it as a priority.

These trends are developments to watch in the next 8 years as they impact cybersecurity threats. They were however, not selected based on their ability to impact cybersecurity but rather on their impact on society as a whole.

[39] (ENISA, Threat Landscape, 2021)

Impact: 1-5 Likelihood: 1-5

POLITICAL TRENDS

P1 The increasing geopolitical influence of ICT providers

Big communication and technology companies have massively expanded their power in recent decades and are increasingly gaining political power (Taddeo, 2017), which also affects other environments like the economy and society. This increasing power amplifies the geopolitical power of communication providers and puts their geopolitical relevance in a new light.

Other categories: Economic

P2 Increased political power of non-state actors

Increasing global interconnectedness will continue to foster interactions between non-state actors beyond the state's capacity to control them, thus challenging traditional governance in multiple ways. The growing role of non-state actors is changing the political environment, influencing economy, society and more. The influence of social movements such as climate marches has increased, affecting political outcomes. New non-state actors such as digital communities, institutions and social media platforms are gaining power and influencing all levels of governance.

Other categories: Economic, Social

P3 The increasing relevance of (cyber) security in elections

With increasing digitization and the use of information and communication technology, there are new influencing factors that can affect election ecosystems. Today's voting ecosystems encompass more than traditional paper-based processes. With new technologies, electoral ecosystems (Petrov, 2018) are becoming increasingly vulnerable to cybersecurity gaps as they offer attackers a larger attack surface. Not only the core electoral systems could be a target, but also election administrators and entities related to the election campaign itself such as political parties, news organizations, social media platforms, email platforms and donor groups are potential targets.

Other categories: Technological, Social

P4 The public health issues arising from the mental health problems of victims of cybersecurity

With the increase of our data on the Internet and the increasing need to use online platforms and digital services, a state of exhaustion in the population could occur due to emerging cyber security gaps. Increasing cybersecurity challenges will lead to greater vulnerability of the general population, resulting in increasing public health risk from cybersecurity.

Other categories: Social

Impact: 1-5 Likelihood: 1-5

POLITICAL TRENDS

P5 Industrial control systems and operational technology networks are increasingly targeted by threat actors

Threat groups are increasingly targeting organizations with industrial control system (ICS) or other operational technology (OT) environments by exploring vulnerabilities. Attackers are increasingly demonstrating high skillsets and a robust understanding of operational technology and industrial control systems engineering and conduct more and more attacks that gain access and negatively impact operations and human safety.

Other categories: Technological, Legal

P6 Increased technological dependency of governments on private sector technology companies

With the current pandemic and ongoing digital transformation, governments are becoming increasingly dependent on private sector technology companies, their products and services. As the power of tech companies increases, some tech companies have more power than some national states. Increasing interdependence between government and companies makes it more difficult to control and identify separations, leading to increased dependence on the private sector, and in many cases single entities within the private sector.

Other categories: Legal, Economic

P7 COVID speeds up digitalization in public sector

In times of a pandemic, when chains of infection have to be traced and everyday processes have to be digitized, the digital transformation of the public sector is accelerating rapidly (ENISA, Raising Awareness of Cyber Security, 2020). The coronavirus pandemic is forcing local governments to offer services online. In addition, e-government technologies such as digital registration offices are replacing human interaction between citizens and government officials with technology.

Other categories: Technological, Social

P8 The increasing digital dependencies and cyber vulnerability of populations

The population increasingly uses technology to manage everything from public services and business processes to private matters and becomes highly dependent on it. Many operations and processes can no longer be managed without technology today and therefore make technology indispensable for the population. The increasing use of digital services and products leads to more personal data that is exposed on the Internet. This reliance on technology on one side and the provision of information on the other side poses a threat and makes the population more vulnerable

Impact: 1-5 Likelihood: 1-5

POLITICAL TRENDS

P9 The growing pressures on a reduced cybersecurity workforce

Mental health can have a critical impact on industry professionals. IT systems are constantly being attacked, so the workload remains high and is relentless. As cyber-criminals innovate new methods of penetrating systems at a fast rate, the challenges to keep up are intense. The European labour shortage in information security means that many departments are operating with half the staff needed which increases stress and pressure exponentially.

Other categories: Social

ECONOMIC TRENDS

EC1 The rise of smart cities

European and global cities are gradually becoming smarter with the use of digital solutions to make cities safer, more efficient and sustainable. Especially countries in the Middle East and Asia have been very proactive in developing smart cities, with a tendency to build them from the ground up while developed cities around the world are actively incorporating technology into existing environments and launching smart solutions. The drive of sustainability and efficiency leverages the usage of technology and data. The aim is to create improvements across infrastructure (ENISA, Guidelines for Securing IOT, 2020), mobility, energy, healthcare and beyond. Sustainable development of urban areas is a challenge of key importance. It requires new, efficient, and user-friendly technologies and services, in particular in the areas of energy, transport and ICT.

Other categories: Technological, Legal

EC2 Use of Distributed Ledger Technologies is growing

Distributed ledger technology, more commonly known as blockchain technology, refers to the technological infrastructure and protocols that allows simultaneous access, validation, and record updating in an immutable manner across a network that's spread across multiple entities or locations. Blockchain technologies have an integral role in the development and growth of new technologies and solutions. They enable interoperability across different virtual platforms, allowing digital collectability of assets and enable digital proof of ownership.

Other categories: Technological

Impact: 1-5 Likelihood: 1-5

ECONOMIC TRENDS

EC3 Non-traditional work structures like freelancing are rising in popularity ("gig economy")

Freelance (or Gig-) Economy refers to a labor market characterized by the prevalence of short-term contracts or freelance work as opposed to permanent jobs (Antonio Aloisi, 2022). The pandemic amplified the popularity of the Gig economy since the current health crisis disrupted many businesses and altered the course of many companies. The current interest in the gig economy has also been spurred by the application of digital technology and the use of platforms. When talking about the gig economy, the subject is usually platform economy—and more specifically platform work. App-based transportation—like Uber, food delivery, or other consumer-facing services—represents particularly visible changes to work and offer flexible working models. The platformization of this work is drastically reshaping the gig economy—with the potential to create widespread impacts across the entire economy.

Other categories: Social, Legal

EC4 Collecting and analyzing data to assess user behavior is increasing, especially in the private sector

An increasing amount of companies have started to monitor, track and follow people in virtually every aspect of their lives. The behaviors, movements, social relationships, interests, weaknesses and most private moments of billions are now constantly recorded, evaluated and analyzed in real-time. Internet of Behaviors (IoB) is the collection of data on the use of gadgets to obtain information on user behavior, interests, and preferences. The data can serve as a benchmark for mapping customer behavior and aims to properly understand and apply data to create and promote products. It will continue to influence how organizations interact with people. IoB can collect, combine and process data from a variety of sources.

Other categories: Legal, Social, Political

EC5 Increasing reliance on automation and connectivity of sustainable energy production

The use of renewable energy will increase over the next decade as EU governments and societies seek to avoid the rising costs, environmental and political impacts of fossil fuel dependency. Accompanying this shift is an increasing automation of equipment used to harvest such energy, such as solar panel arrays and wind generators, by the companies that operate them. The main driver for increasing automation will be to reduce the costs normally associated with the operation and maintenance, such as inspection and repair, of these plants. This increasing reliance on IoT devices to monitor, manage and perform maintenance on assets will expose the EU's energy sector to a variety of cybersecurity challenges.

Other categories: Technological

Impact: 1-5 Likelihood: 1-5

ECONOMIC TRENDS

EC6 Increasing reliance on outsourced IT Services

European IT outsourcing to external service providers has rapidly increased due to the pandemic (Krajewski, 2021). Due to the increasing gap of available IT jobs and the number of IT professionals, there is an increasing need to fill important IT tasks. An option for European companies, which provides flexibility, is to outsource IT tasks to offshore providers. As companies are moving into the cloud (quicker) and need tailor-made solutions, the need for IT professionals increases further. Since the shortage affect most European countries, and most European developers prefer jobs within their own country, companies increasingly recruit talent from outside Europe. The presence of different migrant communities - a so-called diaspora - adds to the diversity of opportunities on the European market. These outsourced providers can be domestic, nearshore or offshore. European companies prefer to outsource services to providers within the same country, a practice also known as domestic outsourcing. When outsourcing abroad, they prefer providers in nearshore locations because of proximity, language, cultural similarities and minimal time differences. As prices in nearshore countries in for example Central and Eastern Europe rise, offshoring to developing countries becomes more attractive.

Other categories: Social

EC7 Increasing danger of resource bottlenecks of critical raw materials for strategic technologies and sectors in the EU

With the increasing use of crucial technology (batteries, fuel cells, robotics and more), maintaining access to vital resources such as energy, raw materials, pharmaceuticals and technological components such as micro-chips is vital for the EU's economic prosperity. The emerging on new technologies in the course of digitization requires new resources to provide hardware for e-cars, sensors or other technologies. Currently, EU industry is largely dependent on imports for many raw materials and in some cases is highly exposed to vulnerabilities along the supply chain.

Other categories: Technological

EC8 The rise of Web3 leverages various emerging technologies incl. blockchain

Web3 is the third iteration of the internet and will be defined by open-source technology, utilizing blockchain technology to be trustless and permissionless. Web3 harnesses blockchain to "decentralize" management thus reducing the control of big (tech) corporations and making it more democratic. With Web3, activities and data would be hosted on a computer network using blockchain instead of corporate servers, based on ubiquitous high-speed access and the development of web-based business applications at the enterprise level. Internet activities would be represented by crypto wallets and websites hosted through decentralised applications, digital applications running on a blockchain network. This enables wireless interaction between machines, vehicles, devices, sensors and many other devices via the internet.

Impact: 1-5 Likelihood: 1-5

ECONOMIC TRENDS

EC9 Internet traffic will triple with increased access worldwide

It is predicted that there will be 6 billion internet users by 2022 and more than 7.5 billion internet users by 2030 (Stackscale, 2021). Even in European countries, internet traffic has increased strongly within the past couple of years and has increased access and traffic in rural areas. Internet traffic has skyrocketed over the past year due to more IoT devices and hence the increased connectivity between devices such as smartphones, wearable technology, automobiles and more. Remote work, video streaming, video calls and online shopping are some of the activities that have grown the most and have contributed to such increase

Other categories: Social, Technological

SOCIAL TRENDS

S1 Advancement of deep fake technology

Deepfake is a combination of the words 'deep learning' and 'fake' and refers to an AI-based technology used to create or alter images, audio, and video resulting in synthetic content that appears authentic (Shein, 2022). With the world more connected by digital media and the costs for creating deepfakes slumping dramatically, this emerging technology is gaining more importance. Deepfakes have the potential to transform different sectors such as education, art, digital reconstruction, public safety and the entertainment industry.

Other categories: Technological, Political, Legal

S2 Decision-making is increasingly based on automated analysis of data

Important decisions that impact human lives, livelihoods, and the natural environment are increasingly being automated. Delegating tasks to so-called automated decision-making systems (ADMS) can improve efficiency and enable new solutions but may also present additional ethical challenges.

Other categories: Political, Legal

Impact: 1-5 Likelihood: 1-5

SOCIAL TRENDS

S3 The rise of brain-computer interfaces

Brain-Computer Interfaces also known as Brain-Machine Interfaces or Direct Neural Interfaces are computer-based systems that acquire brain signals, analyze them and relay them to external devices like IT systems or wearables to translate them into appropriate actions. The ability to detect electrical activity in the brain, and to control it, will change society in profound ways. Patterns of electrical activity in the brain can reveal a person's cognition. New methods to stimulate specific brain circuits can treat neurological and mental illnesses and control behavior. The ability to interrogate and manipulate electrical activity in the human brain promises the monitoring of electrical activity in the brain.

Other categories: Technological, Legal

S4 The rise of digital authoritarianism

The internet is growing less free around the world, and democracy itself is atrophied under its influence. Disinformation and propaganda disseminated online have poisoned the public sphere. The unbridled collection of personal data has broken down traditional notions of privacy. And a cohort of countries is moving toward digital authoritarianism by embracing the Chinese model of extensive censorship and automated surveillance systems. For the first time since 2004, the Transformation Index (BTI) (Stiftung, 2022) counts more autocratically governed states than democracies. Economic and governance performance also show downward trends, with the coronavirus pandemic having exposed and exacerbated existing weaknesses.

Other categories: Political

S5 Exponential increase of digital technologies in everyday life

The increased access to internet and increased traffic through IoT (ENISA, Threat Landscape, 2021), including smartphones and other devices, along with social media platforms and messaging apps, transform many sectors in Europe such as education and learning, making and maintaining friendships, how to spend leisure time, and the engagement with wider society. Along with the benefits comes a diverse range of risks and harms.

Other categories: Technological

Impact: 1-5 Likelihood: 1-5

SOCIAL TRENDS

S6 Online education in the EU grows

The COVID 19 pandemic has led to schools being closed all over the world. While countries are at different points in their COVID-19 infection rates, worldwide there are currently more than 1.2 billion children in 186 countries affected by school closures due to the pandemic. As a result, education has changed dramatically, with the distinctive rise of e-learning, whereby teaching is undertaken remotely and on digital platforms. Even before COVID-19, there was already high growth and adoption in education technology, with global EdTech investments reaching US$18.66 billion in 2019 and the overall market for online education projected to reach $350 Billion by 2025 (Detecon, 2022). The integration of information technology in education will be further accelerated and online education will become an integral component of school education.

Other categories: Technological

S7 Increased democratization and access to AI programming and applications

'AI for everybody' refers to the principle of democratizing Artificial Intelligence (AI) and making related specialist technologies accessible. This way, other people can have access to these tools and can modify this code to integrate it with their products resulting in improved efficiency and increased engagement. Even the most sophisticated AI systems, designed by highly qualified engineers, can fall victim to bias, explainability issues, and other flaws. An AI system built by someone without proper training, or operating without appropriate controls, could create something outright dangerous — introducing discrimination or serious errors.

Other categories: Technological

Impact: 1-5 Likelihood: 1-5

TECHNOLOGICAL TRENDS

T1 There is an increasing popularity of everything as a service (XaaS) demand and supply

Disruptions due to shutdowns and the complexity of rapidly enabling a remote workforce have created the need for flexible IT solutions (Insights, 2022). To keep up in today's rapidly changing environment, organizations need solutions that enable them to create new business processes, products, and services. The adoption of the everything-as-a-service (XaaS) model is increasing and has become an indispensable asset for sustaining businesses. As a result, companies become increasingly dependent on these providers. By hiring offshore software developers, IT suppliers and everything-as-a-service, companies can eliminate office space and reduce all associated costs. The increasing outsourcing of business constantly results in new risks and challenges that increase complexity.

Other categories: Economic

T2 Satellite control infrastructure is increasingly critical

The number of satellites in space is increasing and thus our dependency on satellites (Tim Starks, 2022). With more than 1000 new satellites expected to launch each year over the next year, a robust satellite control infrastructure is gaining more and more importance. GPS is increasingly integrated into sectors' operations such as aviation, railway, maritime operations and other infrastructure because it is accurate, available, reliable, and provided at no cost to users. The ground-based infrastructure for a satellite is responsible for a number of support functions, such as commanding the spacecraft, monitoring its health, tracking the spacecraft to determine its present and future positions, collecting mission data, and distributing these data to users. A key component of the infrastructure is the ground station, which is an Earth-based point of contact with a satellite and a distributor of user data.

Other categories: Political, Environmental

T3 AI-based systems are increasingly deployed with bias or issues that impact inclusivity, safety, ethics, privacy, trustworthiness, and explainability

Machine learning and artificial intelligence are able to process the increasing amounts of data that are generated every second. With the increasing use of AI-based systems, new challenges arise in relation to data ownership, sovereignty, data protection and compliance. Recent examples of algorithmic biases based on gender, ethnicity, or sexual identity in AI technology have demonstrated instances when AI abandon the principles of inclusivity, safety, ethics, privacy, trustworthiness, and explainability. These findings may lead to the massive risk that future societies not only continue to project historical human biases, but also risk exacerbating those biases.

Other categories: Legal, Political

Impact: 1-5 Likelihood: 1-5

TECHNOLOGICAL TRENDS

T4 Extended Reality is going mainstream

XR is an emerging umbrella term for all the immersive technologies. The ones we already have today—augmented reality (AR), virtual reality (VR), and mixed reality (MR) plus those that are still to be created. All immersive technologies extend the reality we experience by either blending the virtual and "real" worlds or by creating a fully immersive experience. Extended reality is going mainstream, benefitting more industries and sectors including digital learning, entertainment, health, manufacturing and more. Extended reality (XR) is becoming more realistic and together with more possibilities to use different applications increase the uptake of the technology. Europe is very strong on the application side and the XR market supports many excellent small and medium-sized enterprises (SMEs) developing high quality software and hardware.

Other categories: Social, Economic

T5 Vehicles are becoming increasingly connected to each other and to the outside world and less reliant on human operation

Cars are becoming more connected to other cars, to transport infrastructure, to pedestrians, and to data centers. With car operating systems running everything from infotainment to autonomous driving, vehicles are becoming ever more intelligent and less reliant on human operation (Todd, 2021). With car operating systems running everything from infotainment to autonomous driving, vehicles are becoming ever more intelligent and less reliant on human operation.

Other categories: Social, Lega

T6 Digital Twins are entering mainstream use

A digital twin is a digital representation of a real-world entity or system. The implementation of a digital twin is an encapsulated software object or model that mirrors a unique physical object, process, organization, person or other abstraction. Due to rapidly evolving simulation and modelling capabilities, better interoperability and IoT sensors, and more availability of tools and computing infrastructure, the use of digital twins increases. As a result, digital twins' capabilities are more accessible to organizations large and small, across industries.

Impact: 1-5 Likelihood: 1-5

LEGAL TRENDS

L1 The increased and improved connectivity of illegal businesses

Criminal groups benefit from the rapid advances in technology, helping them to evade detection and find new markets for their illicit activities, while expanding their reach and malicious impact. The darknet and hardly traceable platforms provide a convenient sales channel or collaboration tool to technologically knowledgeable customers. This approach to weapon and drug sales appears to have considerable potential to grow, as well as the gathering of certain groups. This is especially likely to occur, because platforms like Telegram are easily accessible and provide anonymity and safety for their users.

Other categories: Economic, Technological

L2 The increasing difficulty for law enforcement to access data stored on (encrypted) networks and the use of collected data

The EU agency for law enforcement, Europol (Stolton, 2020), has recognized the increasing difficulty of police authorities in Europe to access data stored on (encrypted) networks, as the EU itself attempts to find legal solutions that will facilitate police access to protected communications. The increasing implementation of technological developments have complicated the ability of law enforcement to gain access to and gather relevant data for criminal investigations. One of the most prominent examples in this regard remains the widespread use of encryption, which contains many benefits from a security perspective but is also a development that criminals have gratefully used to their advantage. New challenges for law enforcement authorities will arise with the gradual onset of 5G in Europe because the technology employs 256-bit encryption that allows for unprecedented levels of privacy and anonymization in mobile communications networks With the increase in volume and importance of cross-border investigations in the EU, ensuring the admissibility of evidence gathered in another Member State at trial is crucial − both for efficient law enforcement and for the protection of fundamental rights. At present, the rules on the collection, use, and admissibility of evidence are left to the laws of national criminal procedure of the Member States. These differ extensively as to the collection, use, admissibility, and nullity of evidence and thereby act as an obstacle to the use of cross-border evidence.

Other categories: Technological, Political

L3 The capacity to control data about oneself (individual, company or state) is becoming more desirable and more technically difficult

With the increasing use of digital products and services, there is more personal or sensitive data on the Internet, which is being tracked, including biometric, genetic, and behavioural information (ENISA, Guidelines for SMEs on the security of personal data processing, 2017). More and more EU consumers are concerned about how their data is being used online and are calling for the ability to not only access and modify their data, but to control the access and usage rights. Since there is no way to own the rights to personal data and to manage access to this data, this becomes technically more difficult for the users.

Impact: 1-5 Likelihood: 1-5

LEGAL TRENDS

L4 Increasing introduction of (technical) legislation in Europe

With the increase in connectivity, digital providers and platforms entering the market are exponentially growing and increasing their influence globally. Ensuring compliance to European standards is becoming an ever more complex task. Europe's competitiveness, technological sovereignty, ability to reduce dependencies and protection of EU values, including social and environmental ambitions, will be evermore challenging. To face this challenge the EU will start regulations/legislation firms and technology more.

Other categories: Political, Technological

L5 Most major technological players continue to reside outside of the EU

Software engineering and digital, data-driven companies form the backbone of the future economy and digital society (Madiega, 2020). In these markets, US and China are by far the biggest players. Besides SAP, Europe does not have any enterprises of comparable strength and only a significantly lower number of startups and venture capital being invested in the region. Moreover, current trends in technology innovation and entrepreneurship intensify this power-imbalance. This means European data is being processed by companies outside the EU.

Other categories: Economical, Political

L6 Rising drive towards EU strategic autonomy

An increasing number of politicians and analysts argue that the European Union should boost its 'strategic autonomy' and/or develop a higher degree of 'European sovereignty'. These concepts encompass a greater potential for independence, self-reliance and resilience in a wide range of fields – such as defense, trade, industrial policy, digital policy, economic and monetary policy, and health policy – following a series of events in recent years that have exposed Europe's vulnerability to external dependencies.

Other categories: Political, Economic

Impact: 1-5 Likelihood: 1-5

ENVIRONMENTAL TRENDS

EN1 The increased usage of new technologies in remote maintenance

With the incorporation of new technologies such as artificial intelligence, sense and avoid systems, and cloud computing in drones, the use of drones for critical infrastructure monitoring and maintenance is increasing. Remote Maintenance describes maintenance, inspection and repair work without personal presence at the object and thus removing the human element from these processes. Drones are being used to perform inspections on critical infrastructure sectors such as blade maintenance in the wind energy sector, roadways and railways inspection or in agriculture.

Other categories: Technological

EN2 Diminishing availability of fresh water

About 70% of the world's freshwater consumption is for agriculture and food demand is rising (Harvey, 2018). The global population is increasing and becoming richer, which will significantly increase global food demand in the coming decades. By 2030, the global middle class is estimated to grow from 2 billion today to 4.9 billion and this will significantly increase the water required for food production. As people move from low income to middle class, demand increases for meat products which have higher water requirements than crops. Other factors that accelerate this trend is the increased frequency of drought due to climate change, increased energy requirements and inadequate water infrastructure.

Freshwater scarcity affects all parts of the environment, society and economy. This leads to crop failures, increased fuel consumption by companies that rely on hydroelectric power, poor soil quality or increased criminal activities such as war, robbery and theft.

Other categories: Social, Economic, Political

EN3 There is an increasing number of devices that are not (or are unable to be) regularly patched

Updates and patching will grow exponentially with the increase in the number of overall devices (Micro, 2019). With the increasing application of IoT, more and more devices are being used, making it more difficult to update all devices in a timely manner. Ability to patch systems being deployed within critical infrastructure without disruptions may also continue to be a problem going into the future.

Other categories: Technological

Impact: 1-5 Likelihood: 1-5

ENVIRONMENTAL TRENDS

EN4 Automation of agricultural skills and workforce

By 2050 two-thirds of the world's population will live in urban areas, reducing the rural workforce. Operations will be done remotely, processes will be automated. A farmer's skills will increasingly be a mix of technological skills and knowledge of biology. The exposure of agricultural infrastructure and operations to a connected environment will lead to challenges in ensuring the security of food supplies. Also, the dependency of farmers on niche technologies increases. New technologies are likely to intensify exploitation and deepen marginalization for most vulnerable.

Other categories: Technological, Economic

EN5 The increasing threat of extreme weather events due to climate change

Statistics in the latest IPCC report show, that there will be an increase in the number of extreme weather events and that these events will become more extreme, causing more damage than previously observed (IPCC, 2022). Also, the EU is expected to experience more extreme events and increased exposure and vulnerability to disasters. Climate change is bringing along more extreme weather events, sea-level rise and changes in the geographical distribution of some infectious diseases. Continued urbanization and development in hazardous areas have been putting more people and wealth in harm's way. Urban settings are vulnerable to even more catastrophic impacts of disasters such as floods, heatwaves or epidemics.

Other categories: Economic, Social, Technological

EN6 Mass extinction and loss of biodiversity continues

Humans alive today are witnessing the beginning of the first mass extinction in 65 million years. Scientists believe that at the current rate, the world could be on track to lose that number within a few centuries. Over the next few decades alone, at least 1 million species are at risk of being wiped out. That's according to an estimate in a landmark report published in 2019. The results of a collapse in biodiversity is complex and can lead to a loss of food security, soil fertility, an increase in water shortages and natural disasters or increase the risk of pandemics.

Other categories: Social

Impact: 1-5 Likelihood: 1-5

ENVIRONMENTAL TRENDS

EN7 The emerging use of distributed and alternative energy resources

Driven by the objectives set out in the Paris Agreement, the cost-competitiveness of renewables and growing demand for sustainability from governments, investors and consumers, renewable energy has become an attractive energy source for businesses around the world. Power grids around the world are becoming more decentralized, resulting in distributed energy resources (DER) that are transforming energy markets. The DER (SAP, 2022) market has expanded annually by double digits, with the greatest gains coming from sales of power storage equipment, photovoltaic systems, and systems that manage energy and the response to demand. And recent policy moves—including new energy savings policies in the European Union—will likely further fuel demand from businesses in the DER segment.

Other categories: Economic, Technological

EN8 The increasing energy consumption of digital infrastructure

Digitalization describes the growing application of ICT across the economy, leading to increasing volumes of data, progress in advanced analytics, and greater connectivity between humans, devices and machines (IEA, 2017). Digital devices potentially offer improvements in energy efficiency. This long-term trend towards energy efficiency is counteracted, by the rebound effect. More people streaming videos for a longer period of time require greater amounts of energy and therefore emit more CO2 as a result. The same applies to audio data, images or the video conferences, which causes large increases in energy use. The increasing use of the oldest and most well-known cryptocurrency, Bitcoin, guzzles energy due to its special consensus algorithm and hence adds to an increase in energy use.

Other categories: Technological

EN9 Industrial switch from fossil fuels to hydrogen or electric (demand)

A growing number of companies in Europe and elsewhere are switching to renewable energy for their manufacturing plants, stores and office facilities. One of the main drivers behind companies' decision to go "green" is to reduce the environmental impact of business operations by cutting down their greenhouse gas emissions.

MAINTAINING AN EMERGING THREAT LISTING

The emergence of new threats is complex, fast-paced, and sometimes unpredictable given the rapid influx of cyber incidents. This exercise should therefore be repeated in a few years to account for changes to the threats and general societal changes. In many cases the likelihood of occurrence and relevance of the individual threats may change suddenly, due to sudden innovations, societal changes or other unforeseeable incidents. Hence, it is recommended to define and implement a process to maintain a listing of emerging threats and to monitor the threats presented in this report.

For most organizations looking to identify their own specific threat landscape for the future, we recommend breaking it down into three workstreams: data collection, collaborative analysis, and synthesis[40]. Data collection takes place throughout the year, the latter two workstreams will need to occur close to one another with a timeline of approximately one month.

4.2 DATA COLLECTION (AKA HORIZON SCANNING)

Throughout the year, a group of individuals briefed on the previous project will collect evidence of new trends, events, or drivers of change that alter the analysis (emergence of a new trend or changes to the threat's likelihood). The data collection should be tackled on a centralization data platform to collect events and trends. The database should be open access and trend information can be from other trend reports, scientific papers and journals, vulnerability warnings from vendors, media reports or internal trend intelligence etc. Where possible, trends or new information may come from other sources such as hackathons, simulation games, or consumer protection organizations. The best information is gathered by a large and diverse community with varying perspectives.

The data collected do not necessarily need to be trends – it may be events with the potential to create new threats or alter existing ones, like technological disruptions (e.g. operationalization of deep fakes), political destabilization / stabilization (e.g. expansion of Ukraine conflict to other European nations), etc.

Data points may include sudden crises – these would not be analyzed as a part of this process. There is, however, a recommended process for innovative shorter-term planning in ENISA's Foresight Challenges report.

4.3 COLLABORATIVE ANALYSIS

Once a year, a workshop takes place to discuss collected trends or events that could alter the threat analysis with experts from PESTLE dimensions and cybersecurity. Because of the interdisciplinary nature of the context of the trends (PESTLE), it is recommendable to have a workshop with experts from each PESTLE-dimension and also cybersecurity experts. The people chosen to participate in this workshop should be involved in the ongoing data collection – this ensures continuity and commitment.

[40] (ENISA, Cybersecurity Threat Landscape Methodology, 2022)

4.4 SYNTHESIS

The final stage is taking the findings from the workshops and comparing them with the previous threat report. The listing should then be updated with qualifying justifications why a new threat has emerged, changed, or been removed.

A METHODOLOGY

Based on the use case titled "Identification of Future and Emerging Challenges,[41]" described on page 32 of ENISA's 2021 report on Foresight Challenges, the methodology for this exercise was designed to identify relevant transformations, document possible future states, and to identify drivers of change and threats for the year 2030. To ensure that the aims of the exercise were in accordance with ENISA's specifications and proposed timeframe, the approach described for the use case had to be modified, reducing the activities in scope and complexity. Additionally, a structure to manage the large amount of researched information and collected knowledge on the future had to be developed, to support the methodology. Both proposed amendments to the framework were aimed at reducing the time of execution to five or six months, as opposed to one year.

Figure 6: Identification of future and emerging challenges use case, as defined in the ENISA Foresight Framework

Category	Description
Objective	Produce an overview of emerging trends and challenges that will impact security (report)
Time Horizon	3 -5 years
Collaborating Stakeholders	ENISA Working Group & Broader Public
Target Audience	General public, policymakers, cybersecurity professionals
Impact on Target Audience	Stay up to date on future and emerging challenges; think critically about the future
Level of Granularity	General trends, directions, and topics.
Time to Conduct Exercise	1 year
Dependencies	Other ENISA activities rely on this study

Defining the goal and framework of the foresight project is fundamental to the exploration and research of trends. Therefore, the project's time horizon was defined as 2030 and the stakeholder scope was EU cybersecurity-relevant positions. Based on this scope, the project

[41] (ENISA, Foresight Challenges, 2021)

followed the approach of trend exploration and prioritization, threat identification and their prioritization, and delivery.

In the exploration phase, the working group reviewed various sources and materials on trends. Experts from each PESTLE dimensions reviewed, discussed and prioritized those trends, which then defined the basis of the scenarios used for the threat identification and prioritization[42]. A diverse foresight expert group reviewed and explored possible threats inside these scenarios by using the method “Science Fiction Prototyping”. As last step, cybersecurity experts discussed and prioritised those threats as final delivery for the report.

This chapter is a description of how the ENISA project team defined key terms within the project. It will also help to establish a common vocabulary with the reader.

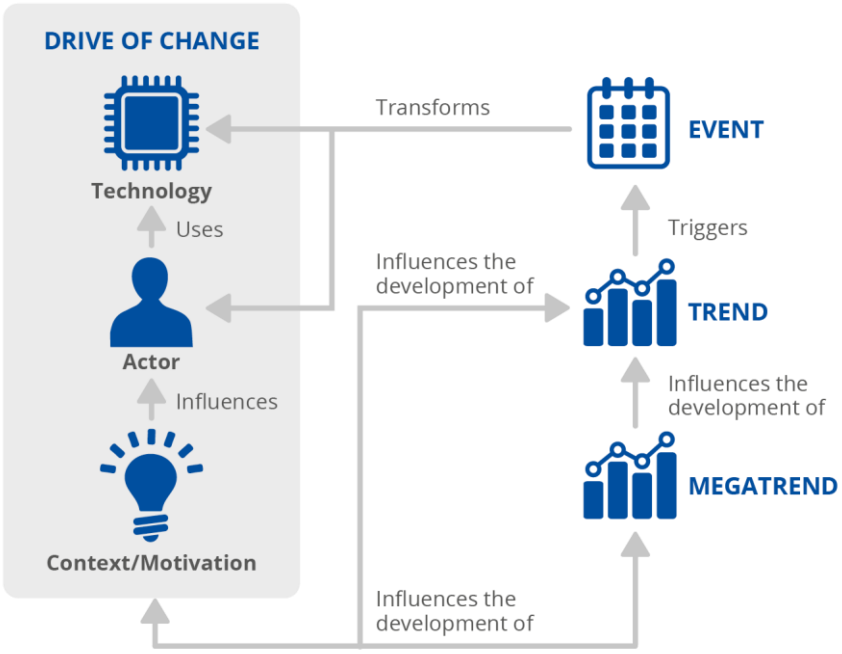
[42] (West, 2017)

B FORESIGHT INFORMATION MODEL

Dialogue, conversation quality, and engagement are the means by which ideas, experiences, knowledge, beliefs, assumptions, and tendencies are shared throughout a foresight project.[43] The creation of information and knowledge on the future requires foresight practitioners to unify two different perspectives, one based on data and what can be proven, and one based on ideas and perceptions.[44] The team conducting this exercise observed an increase in the time required to reach consensus when the participants lacked common ground or structure in their interaction.[45]

To address the inherent issues associated with dialogue in foresight, the team crafted a predefined information model. Although information models are most commonly associated with software development practices, the team agreed that the use of a such a model could reduce the variability of concepts during conversations and provide a shared space[46] for the exercise participants to synchronize their perceptions and ideas on potential futures. The information model contains seven clearly defined entities used in foresight conversations, as well as the focused relationships between each entity.

Figure 7: Foresight entity and relationship model



The basic entities of the model are megatrends, trends, events, technologies, actors, context, and motivation. Drivers of change, the combined entity, arises from the combination of technology, actor, and context or motivation. The definition of each entity and the elements it contains are described in the table below.

[43] (Chermack, 2011)
[44] (Wack, 2014)
[45] (Fosnot, 1996). "Scaffolding" is a concept proposed by Lev Vygotsky, which argued that the most effective learning occurs when the learner and the expert jointly construct meaning (of an experience) through dialogue, thus drawing the learner out to the potential level of performance.
[46] (Schrage, 1999)

Table 4: Foresight entities definitions

Entity	Description
Megatrend	A shift in behaviour or attitude that has a global impact and crosses multiple industries.[47]
Trend	A general tendency or direction of a development or change over time. A trend may be strong or weak, increasing, decreasing, or stable. There is no guarantee that a trend observed in the past will continue in the future.[48]
Event	A noteworthy happening involving social or natural actors[49]
Actor	A party that takes part in an affair or event. A stakeholder in the operating environment.
Motivation	The underlying reasoning and drive for the actions of actors
Technology	The technological components leveraged by actors to accomplish their goals
Driver of Change	A combination of elements influencing the development of trends that trigger events.

B.1 TREND DESCRIPTION

During the research phase of this project, trends were documented as follows:

Table 5: Structure of Trend Description

Name	Description
Trend name	A short name for the trend
Trend description	A short description of the trend contains actor(s) and technology(ies) involved
Trend pervasiveness	A qualitative assessment of the pervasiveness of a particular trend in the operating environment/ in a particular PESTLE dimension.
Megatrend relationship	The megatrend (if available) which causes the development of this trend
Associated events	A list of events (non-exhaustive) known or predicted to be triggered by the trend.

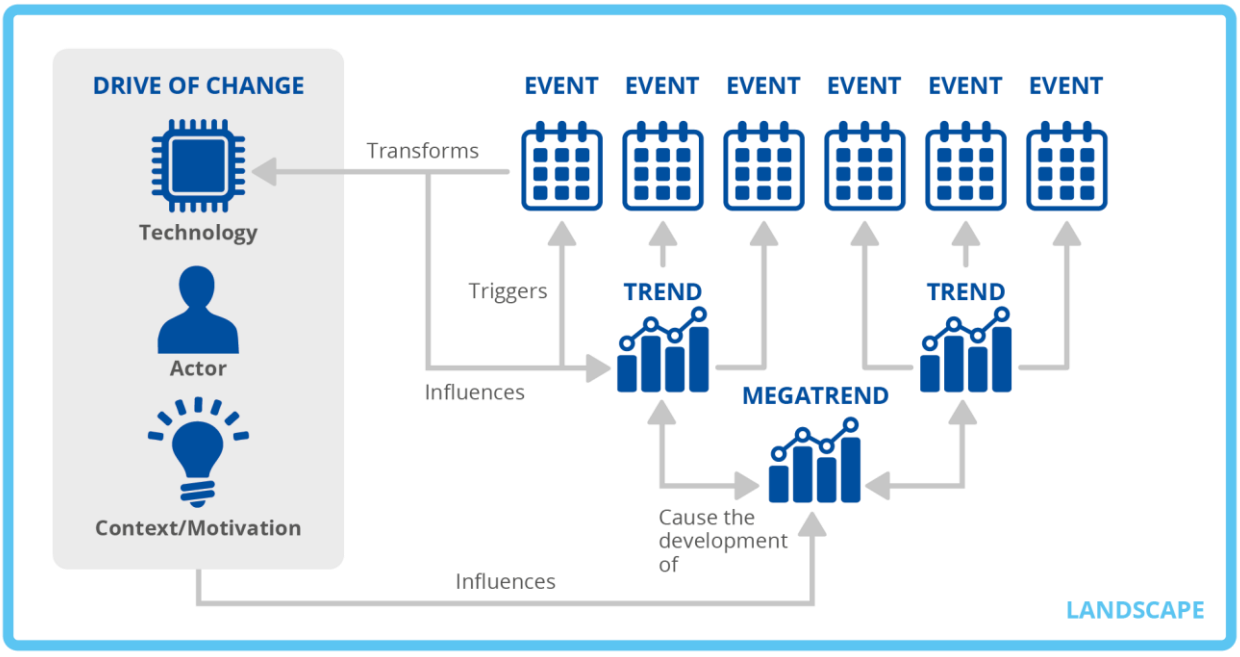
[47] (Popova, 2017)
[48] (Platform, Megatrend / Trend / Driver / Issue, 2014)
[49] (Qualitative Social Research, 2012)

Associated threats	Related threats associated with this trend
Reference documents	The documents where this trend was found, or which was used to define this trend.

B.1.1 Drivers of Change

Drivers of change are the interaction between structural features, institutions and agents, which enables context-specific foundational factors that affect the capacity for reform and opportunities for change. Therefore, the project team analysed trends and events for technology, actors and context or motivation, which have a power relationship or an influence and shaping trends or events.

Figure 8: Landscape of the Drivers of change



B.1.2 Megatrends

A shift in behaviour or attitude that has a global impact and crosses multiple industries.[50] Megatrends are defined as large, social, economic, political, environmental or technological change that is slow to form. Once in place, megatrends influence a wide range of catalysts, activities, processes and perceptions, both in government and in society, possibly for decades. They are the underlying forces that drive trends.[51]

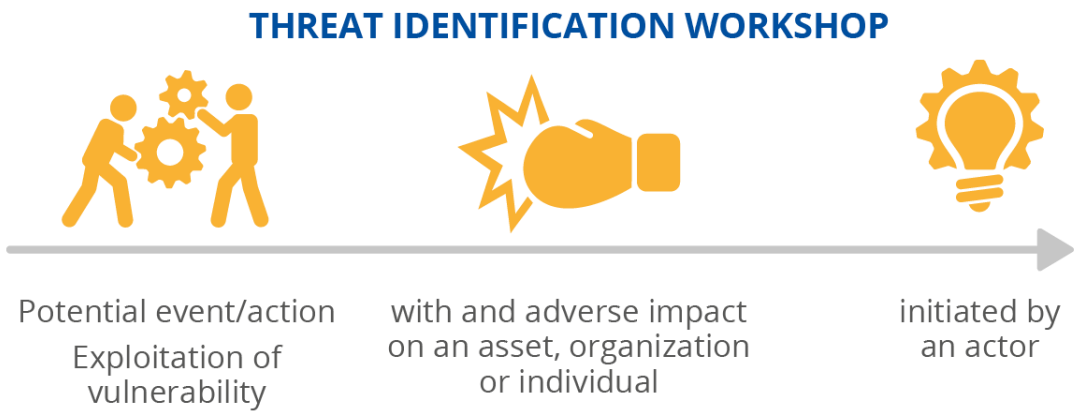
As mentioned above, catalysts play an important role in the landscape of trends. Catalysts are trends accelerating or deaccelerating megatrends, as defined by the ESPAS.[52] The catalysts impacting the cybersecurity sector were aligned with the trend list and their impact on acceleration was discussed with the PESTLE workshop participants.

[50] (Popova, 2017)
[51] (Platform, Megatrend / Trend / Driver / Issue, 2014)
[52] (ESPAS, 2022). Chapter 2

B.2 THREAT ANATOMY MODEL

This section will describe the methodological aspects and entities related to the threat anatomy model used in later process stages of the framework to describe threats in the year 2030.

Figure 9: Threat anatomy model



The team defined a threat as a potential event or action, with an adverse impact on an asset, organization or individual initiated by an actor. This definition was derived from ENISA's, CISA's[53], and CompTIA's organizational definitions of threats.

The potential event or action could be the exploitation of a vulnerability. A vulnerability in this context was defined as any system, structure, asset, or population particularly open to attack or damage. The second characteristic of the threat definition was adverse impact. The team did not provide any pre-defined impact categories to avoid limiting the workshop participants' creativity in identifying the potential impact. Examples of adverse impact were disruption (of services), financial or physical damage, breach of privacy or decreasing trust of citizens. For the third part of the definition, the team asked the workshop participants what part of society would be impacted by the event. Neither of the affected subjects or objects (asset, organization or individual) were defined narrowly. An asset, therefore, can be understood as anything with value – whether that is a technical or intangible asset. An organization could be a private company or a governmental organization. The last element of the threat definition was the threat actor, for which the team had not defined any categories like state-sponsored actors, criminal groups, or hackers-for-hire. These categories were added to the threats after the threat identification workshops took place and were combined with potential motivations of the specified threat actor.

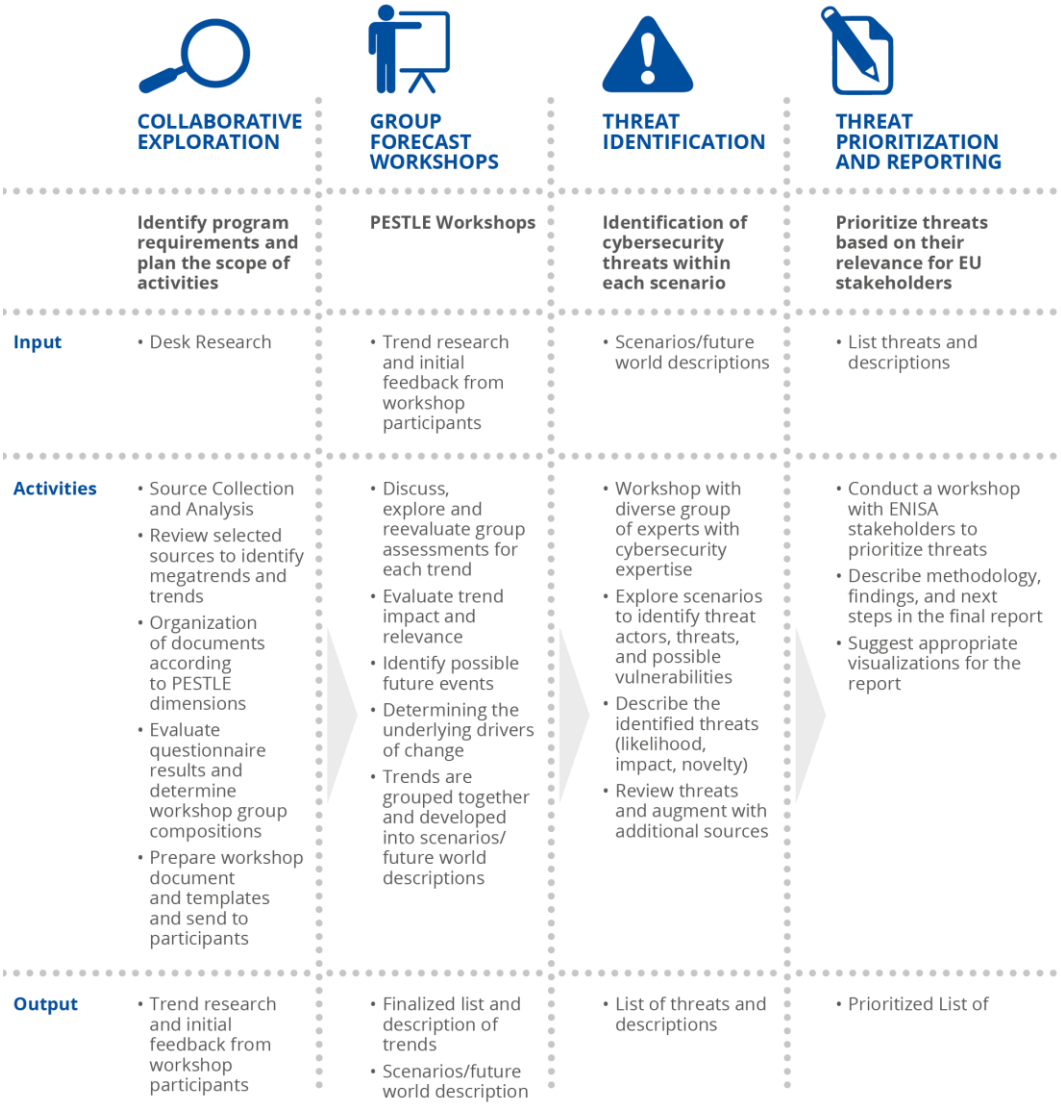
[53] (ENISA, Glossary of Terms., 2018)

C TREND ANALYSIS

C.1 APPROACH & PROCESS

As previously introduced, the team identified four key steps to identify cybersecurity threats in the year 2030: collaborative exploration & scoping, group workshops to forecast future developments based on trends[54], the identification of threats related to the future developments and a prioritization of the threats to be explored. These four process steps were documented, along with the required activities associated to each one into an approach to conduct the exercise. Stakeholders from ENISA's Ad Hoc Working Group for Foresight reviewed and provided input on the planned approach.

Figure 10: Detailed approach for exercise



The approach is iterative in nature, incrementally building up knowledge and information during each phase. This aggregate approach to constructing information on potential futures allowed

[54] (West, 2017)

the team conducting the exercise and the participants to unlock new perspectives at each process step, opening exploration of relevant concepts through focused questioning.

C.1.1 Expert Participant Analysis

Experts who participated in this project (especially in the PESTLE trend workshops) were individuals in ENISA's Ad-Hoc Working Group on Foresight[55] and the Ad Hoc Working Group on Cyber Threat Landscapes. The experts who took part in the Threat Identification Workshop and the Threat Prioritization Workshop were from EU CSIRTs Network and EU CyCLONe – the Cyber Crises Liaison Organisation Network and ENISA stakeholder groups.

The experts interviewed as a part of this project represent a diverse group of individuals. All stakeholders of ENISA's, all participants had expertise in foresight, one of the PESTLE [56] framework elements, and/or cybersecurity. Together they represented 19 EU Member States.

Figure 11: Geographical Distribution of Experts

Participants included individuals from academia, the European Commission, the EU Incident Response and crisis management community, and national-level experts.

C.1.2 Collaborative Exploration

Once the approach was agreed upon, the first phase of the exercise targeted the identification of general trends and analysis of interactions and influences of those trends on cybersecurity. This research involved multiple evaluations of aspects included within the PESTLE framework (Political, Economic, Social, Technological, Legal, Environmental), and exploration of trends, key factors, and other forces that have an evident influence on each of the PESTLE dimensions.[57] The PESTLE dimensions provided a strategic, straightforward, and efficient structure to conduct the analysis. We structured this research into three steps: collection & preparation, collaborative exploration, and finalization. In the first step, we collected research documents, reports, and studies from various sources, such as internal trend studies, open-source studies, reports, publications of government sources, trend research agencies,

[55] (ENISA, Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges, 2021)
[56] (ENISA, A trusted and Cyber Secure Europe, 2020)
[57] (Chermack, 2011).

cybersecurity companies, and consultancies. For each trend, a minimum of two reliable sources was required for it to be added to the list.

The ENISA project team carried out the in-depth review to challenge the relevance and description of each trend and to identify the trend pervasiveness, possible megatrend relationships, and associated events. The decomposition into the determining characteristics ensured a comprehensive basis for the experts' assessments. This list of approximately 120 trends formed the basis for the foresight workshops. Experts invited to PESTLE workshops were provided the list for feedback and preparation.

Group Forecast Workshops

The approach used for the second step – collaborative exploration – utilized expert panels in the form of six workshops, one for each PESTLE dimension. Organizing ENISA's efforts by PESTLE dimensions and performing joint exercises leveraged the power of group dialogue and knowledge. Each dimension involved five participants, who are academics, foresight, and consulting experts from the fields of the corresponding PESTLE dimension, to ensure an adequate mix between the wealth of opinions and efficiency.

In the interactive workshops, facilitated with the online collaboration tool Mural, the approach of the diamond process[58] was followed, divided into three steps: trend exploration and analysis, prioritization, and exploration of prioritized trends. In the first step, the participants were debriefed on the objectives of the workshop and the project and were then asked to review the gathered information on trends. They then provided feedback and discussed, augmented, explored, and extended the list of trends. As a part of this step, the group explored and discussed possible future events triggered by the trends and possible drivers of change.

This phase elicited many valuable insights and information on emerging trends. In order to prioritize the trends, each participant voted for their top three trends, based on their opinion and experience. Then, as a group, the participants were invited to assess the likelihood of occurrence and potential impact on corresponding PESTLE field on a prioritization matrix.

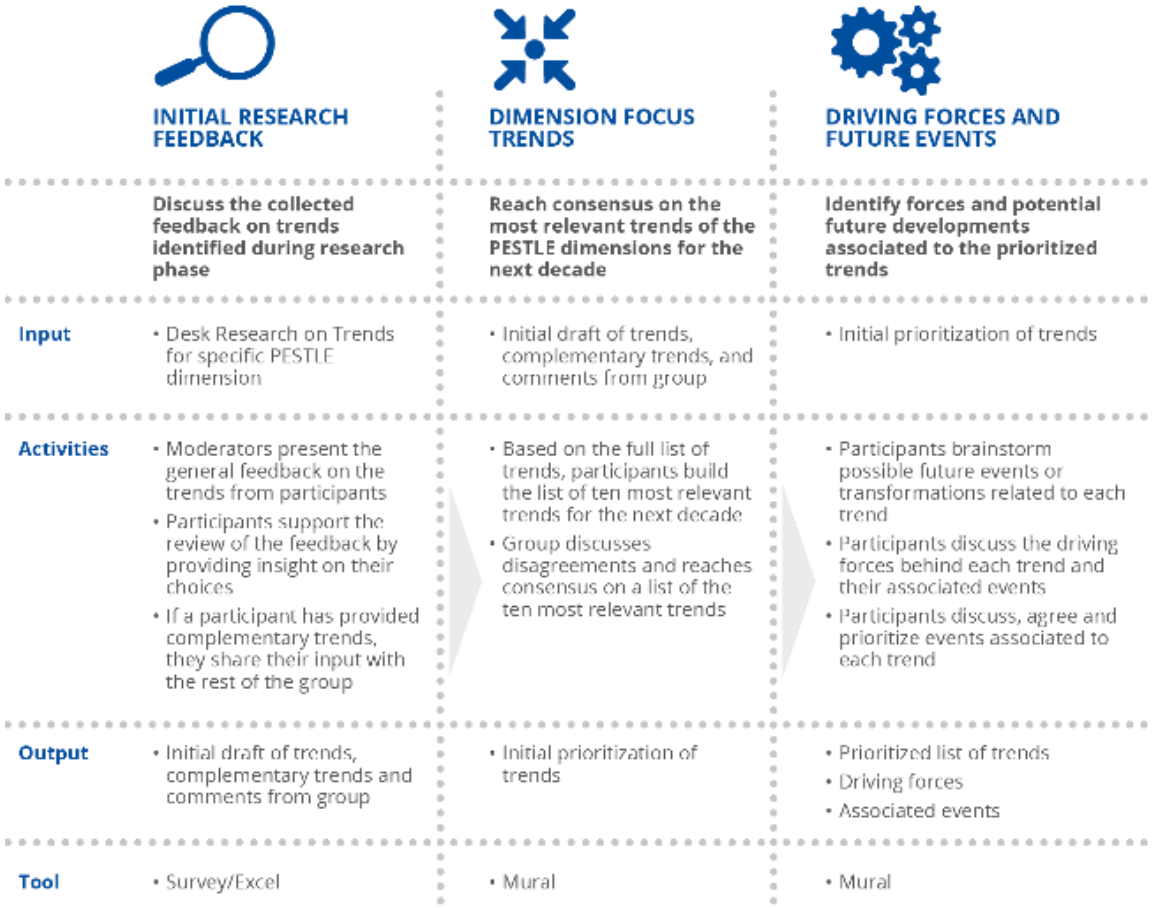
[58] (Thomas Grisold, 2022)

Figure 12: Example of workshop trend prioritization board

In the second task of the workshop, the participants were invited to consider corresponding events that each prioritized trend may trigger in the future (or has triggered already), possible underlying drivers of change (actors, technology, and relevant context), and the elements that may contribute to an increase of the trend's priority (likelihood, impact).

Following the workshops, we initiated the synthesis of all written results on the collaboration tool and the discussions. The experts' discussions also revealed clusters and connections beyond the iteration of all descriptions, events, and underlying forces.

Figure 13: Detailed approach for trend identification & prioritization workshops



D THREAT IDENTIFICATION

For the identification of future threats, the team drew on the threatcasting methodology. Often used by military strategists, threatcasting is a (2011) foresight methodology[59] that draws from traditional futures studies and military strategic thinking. The first phase of threat casting consists of synthesizing research and identifying trends. This part was concluded with the explorative research and the following PESTLE expert workshops.

D.1 SCENARIOS

The next phase in threatcasting is futurecasting, which includes the compilation of the research data into a model of the future environment. The goal of the next step was to simulate possible futures and for workshop participants to immerse themselves as deeply as possible within that future. Using the insights and documented information from the PESTLE workshops, the project team prepared and validated a pared down list of trends from which to build scenarios. The grouped trends and driving factors were crafted into written scenarios to be evaluated by a group of cybersecurity professionals.

Scenarios are consistent and coherent stories that illustrate visions and simulate a possible and plausible future. In times of uncertainty, innovation and change, the use of scenario planning techniques becomes increasingly important because of their usefulness when facing ambiguity and complexity. Scenario planning stimulates strategic thinking and helps to overcome the limitations of thinking[60]. They are not meant to be an exact and realistic representation of the future - they serve to open the field of vision and to uncover blind spots to discover possible futures. This scenario development method helped avoid any bias or selection based on impact or priorities. To design the scenarios, the project team numbered the trends that were prioritized by the experts in the PESTLE workshops and decided to develop scenarios based on 5 randomly selected trends.

Each scenario combined the trends and defined a storyline of a possible future.

D.1.1 Scenario 1 – Blockchain, deepfakes, & cybercrime in a data-rich environment

In 2030, distributed ledger[61] (blockchain) technology has evolved, thus enabling simultaneous access, validation, and record updating in an immutable manner through a network spread over multiple entities or locations. This technology enables interoperability across different virtual platforms, allowing digital asset collectability and digital proof of ownership. Blockchain technology has found widespread use in the financial, logistics, science, and health sectors. It significantly impacts the economy by increasing consumer trust and processing efficiency because of its decentralization.

On the other hand, criminal groups have also benefitted from technological advances, such as distributed ledger technology (e.g. crypto), the darknet, and privacy-focused platforms. New technology is used to widen the groups' negative impact, expand their activities' overall reach, and use technology for sales and collaboration. This development has a major impact on the legal sector.

Deep fake technology is also widely established and accessible to everyone; it enables the creation of synthetic content that appears to be authentic. This technology's mainstream use and distribution will transform sectors such as education, art, digital reconstruction, and the

[59] (ENISA, Cybersecurity Threat Landscape Methodology, 2022)
[60] (M. Stojanovic, 2015)
[61] (ENISA, Blockchain, kein Datum)

entertainment industry. However, its psychological effects will have a major impact on public safety, election processes, and the spread of disinformation.

While technological options for privacy are available and widely used, the private sector is highly dependent on using real-time analysis of customer data from various platforms and sources to create and promote products and understand customer behavior and needs. The data is constantly recorded, evaluated, analyzed and combined, and processed from various platforms and sources. Organizations using this method widen their power and have a big impact on the economy.

In addition to the widespread collection of customer data, organizations collect data from infrastructure components via technologies like IoT and drones and analyze it with AI. With this information, organizations perform inspections, predict failures, reduce workforce requirements, and maintain (critical) infrastructure. This practice has a significant impact on companies in the wind energy, logistics, insurance, roadway, railway, and telecommunication sectors.

D.1.2 Scenario 2 – Eco-friendly, sustainable, and interconnected smart cities (non-state actors)

As the global population rose and became more prosperous, and the frequency of droughts increased due to climate change, the diminishing availability of freshwater in 2030 is posing challenges to all parts of the environment, society, and economy. Crop failures, poor soil quality, increased fuel consumption, and dependency on hydroelectric power increased[62], which led to very high costs of living and an increase in poverty. Consequently, the level of criminal activities including aggressions, robberies, and theft rose dramatically. The increasing energy requirements and the construction of adequate water infrastructure for the new needs are an integral part of planning future cities.

As part of the reconstruction of cities, sectors of infrastructure, mobility, energy, ICT, and healthcare are actively incorporating technology into their existing environment and using data for decision making and improvement. Smart cities create safer, more efficient, and sustainable cities that are adapted to the environmental requirements of climate change. However, the increased use of digital technology into the cities' infrastructure also increased their technological dependence.

With the increasing connectivity and possibilities to collaborate, the political power of non-state actors has continued to grow – broadly impacting both the economy and society. Digital communities, institutions, and other actors are beyond the capacity of the state to control, influencing all levels of governance and changing the political environment. In the communication sector specifically, telecommunication providers[63] have amassed significant geopolitical, economic, and societal power. Furthermore, as all digitalized processes and services are dependent on connectivity, both local and transcontinental communication providers are gaining importance in Europe due to their use of new technology like space connectivity and drones.

The new factors mentioned above have also affected election ecosystems. Core electoral systems are being targeted by digital communities, institutions, and actors. However, the scope of vulnerable components also include election administrators, political parties, news organizations, social media platforms, email platforms, and donor groups – all of which have become part of broader campaigns to manipulate democracy and call into question the trustworthiness of elections.

[62] (IPCC, 2022)
[63] Please note that telecommunications providers will not be the only groups amassing huge amounts of power – the greatest power shift will be towards content providers and hyperscalers.

D.1.3 Scenario 3 – More data, less control

The massive collection and use of data is driving innovation and decisions in all sectors. Important data-driven decisions that impact people's lives, livelihoods, and the natural environment are automated in 2030. The delegation of tasks to automated decision-making systems with little or no human intervention enables new solutions and improves overall efficiency. On the other side, society, and especially sectors like the medical diagnostics sector, the industry of autonomous vehicles, and financial institutes (to issue loans and credit cards) are fighting ethical challenges. Data-based and automated decision-making could lead to discriminatory and biased outcomes, privacy violations, and the undermining of human self-determination.

(IoT) devices are the predominant vehicle for decision-making data. In 2030, organizations using these devices face problems with patch management; it is especially difficult for critical infrastructure[64] providers to update the large number of devices without disruptions or breaches.

With the increasing use of digital products and services, more personal or sensitive data is available on the Internet. This data includes biometric, genetic, and behavioral information and is tracked across different online platforms. Unfortunately, data breaches, attacks, and online bullying have become part of daily life and impact most EU citizens. This results in a severe public health risk; victims struggle with PTSD, burnout, anxiety, depression, abuse, or even suicidal behavior. More and more EU consumers are concerned about how their data is being used online and are calling for increased control over data access and usage rights.

On the other hand, law enforcement has difficulties accessing stored data or using collected data because of the implementation of end-to-end encryption of communication channels, compliance with data privacy regulations, lack of technical capabilities. The implementation of technological developments has complicated the ability of law enforcement to gain access to and gather relevant data for criminal investigations. The widespread use of encryption, which contains many benefits from a privacy and security perspective, is also a development criminals are using to their advantage.

D.1.4 Scenario 4 – Sustainable energy, automated/short-term workforce

In 2030 the use of renewable energy has increased as EU governments and societies seek to avoid the rising costs and environmental and political impacts of fossil fuel dependency[65]. Many organizations automate equipment to harvest such energy, such as solar panel arrays and wind generators. These organizations rely on IoT devices to monitor, manage, and perform maintenance on these assets. This is exposing the EU's energy sector to a variety of cybersecurity challenges.

As more people move to urban areas, the agriculture sector is automated because of insufficiently available workforce in rural areas. This leads to increasing dependency on technology and specialized skills and knowledge to manage agricultural output of countries. The exposure of agricultural infrastructure and operations to a connected environment leads to challenges in ensuring food security for the population of EU countries.

With the shortage of skilled workers, non-traditional, flexible work structures like freelancing have become the norm (e.g., workers in the Gig-economy)[66]. The labor market is characterized by the prevalence of short-term contracts or freelance work as opposed to permanent jobs. The platformization of work drastically reshapes the labor market, with an extreme gap developing between high and low educated people and their income.

[64] (Allianz, 2016)
[65] (Union, 2022)
[66] (Global, 2022)

With the need for flexibility and enabling a remote workforce, organizations increasingly require IT solutions that enable them to create new business processes, products, and services. To increase efficiency and reduce costs, the adoption of the everything-as-a-service model is highly popular and has become an indispensable asset for sustaining businesses. As a result, companies have become increasingly dependent on these software service providers.

D.1.5 Scenario 5 – Legislation, bias, extinctions, & global threats

In 2030, the world's population counts 8.5 billion people, with urban growth taking place in regions relatively undisturbed in the last century[67]. Urban expansion, tropical deforestation, and land-use change sped up mass extinction and the loss of biodiversity. This has caused the loss of food security, soil fertility, an increased water scarcity in Europe. Natural disasters and pandemics have become commonplace.

The internet, once a medium of freedom and expression has increasingly become regulated and censored, democracy itself has atrophied under its influence. Disinformation[68] and propaganda disseminated online have poisoned the public sphere and dialogue. The unbridled collection of personal data has broken down traditional notions of privacy. Moreover, a cohort of countries are moving toward digital authoritarianism, by embracing extensive censorship and automated surveillance systems. Europe, targeting to protect its values, has tried to strengthen its technological sovereignty, by reducing dependencies and including social and environmental ambitions within its technical legislation. One technology already regulated in 2024 is machine learning and artificial intelligence, which is massively invested in. However, with the use of AI-based systems, Europe is being challenged with problems and incidents on data ownership, sovereignty, data protection, and compliance, especially with algorithmic biases. These biases, based on gender, ethnicity, or sexual identity in AI technology, led to the continuing historical human biases and the exacerbation of those biases in societal practices.

Space has also become the main focus of governments and private investment, as space technologies, data and services advanced in the 20s. But the dependence to this critical space infrastructure in space and on the ground made Europe more vulnerable to both manmade and natural threats.

D.2 SCIENCE FICTION PROTOTYPING (SFP)

Science Fiction Prototyping is a "thought-provoking method for arousing discussion in research and foresight of emerging technology.[69]" Science fiction prototypes (SFPs) are stories that allow the workshop participants to explore a wide variety of futures and a different angle on these futures. The SFP is based on a future (scenario), derived from five randomly picked trends and a character (persona) in this scenario, to emphasize this specific point of view[70].

From these models of different future environments, the five groups, each containing two to three cybersecurity experts, were assigned one future model. Based on this model, the group derived one persona and wrote a science fiction prototype (SFP), focusing on the layered effects the future environment has on their persona. To characterize this person, the group imagines a specific person living in that future of the scenario. The group visualizes in a persona template who the character is, their questions, problems, goals, motivations and a possible statement. This step was prepared by the participants and the project team before the workshop[71].

The preliminary work of science fiction prototyping created the basis for the Threat Identification workshop, where the groups moved their focus from the models of the future environment and

[67] (Nations, 2022)
[68] (ENISA, Threat Landscape, 2021)
[69] (Kymalainen, 2016)
[70] (Johnson, 2011)
[71] (Institute, 2021)

their persona to the sphere of cybersecurity threats. The participants explored and discussed cybersecurity threats that included the different layers of their science fiction prototype. Based on the threat definition – a potential event or action with an adverse impact on an asset, organization or individual, carried out by an actor – the groups formulated and defined different cybersecurity threats of the future.

These views of the future are effects-based models, meaning that the group is not modelling a specific threat first; they are exploring the layered effects that this future will have on a single person, related and an active part in this scenario. This creates a more detailed effects-based model that ultimately helps the participants to find more threats but also opens the threat definition in broader depth.

The moderators of the project team guided the discussion with questions and, if necessary, randomly drew Security Cards that served as input for the threat discussion to explore more layers of potential threats. Security Cards were created by the University of Washington in 2013 and aim to foster creative thinking on cybersecurity threats. There are four dimensions within the Security Cards – human impact, adversary's motivations, adversary's resources, and adversary's methods[72]. The Security Cards were drawn by the moderator if the discussion stalled, and the participants were unable to identify new threats. The moderator also encouraged the group to switch perspectives and look at the future environment from the adversary's position to identify more threats.

The output of the Threat Identification workshop was a long list of future cybersecurity threats and their descriptions.

D.3 THREAT PRIORITIZATION

The final step of the process was the conduction of a Threat Prioritization workshop with ENISA stakeholders, refining the threat descriptions based on ENISA cybersecurity expert's feedback to the threats and compiling the identified future cyberthreats into the report at hand. The Threat Prioritization workshop's goal was to rank the threats based on their impact, likelihood, novelty and, therefore, importance for ENISA. Novelty was included to prioritize threats that are not often included in public discourse. This was done in a workshop with ENISA cybersecurity experts, leading to the emerging cybersecurity threats for 2030 list. (See chapter 4.) Impact and likelihood were rated on a scale of 1 to 5; these were multiplied to create a baseline score. Then 2 points were added if the threat was deemed novel; 2 points were deducted if the threat had already been published in another ENISA publication.

After receiving this feedback, the project team refined the threat descriptions and added the actors, methods, and impact category to each top-ten threat.

The threat information may be found in chapter 4 and the scoring for the top 10 threats is in Annex E.

[72] (TAMARA DENNING)

E THREAT SCORING

#	Name	Impact	Likelihood	Impact x Likelihood	Novelty	Previously Published	Total Score
1	Supply chain compromise of software dependencies[73]	5	5	25	+2	-2	25
2	Advanced disinformation campaigns[74]	4	5	20			20
3	Rise of digital surveillance authoritarianism / loss of privacy	4	5	20		-2	18
4	Human error and exploited legacy systems within cyber-physical ecosystems[75]	4	5	20		-2	18
5	Targeted attacks (e.g. ransomware) enhanced by smart device data[76]	4	4	16	+2		18
6	Lack of analysis and control of space-based infrastructure and objects.	4	4	16	+2		18
7	Rise of advanced hybrid threats making use of different and unforeseen modus operandi (e.g. disinformation)[77]	4	4	16		-2	14
8	Skill shortage78	4	4	16		-2	14
9	Cross border ICT service providers as a single point of failure	5	3			-2	13
10	Abuse of AI	4	3	12	+2	-2	12

[73] (ENISA, Understanding the increase in Supply Chain Security Attacks, 2021)
[74] (ENISA, Threat Landscape, 2021)
[75] (ENISA, Threat Landscape Report, 2022)
[76] (ENISA, Personal Data Breaches, 2020)
[77] (ENISA, A trusted and Cyber Secure Europe, 2020)
[78] (ENISA, Raising Awareness of Cyber Security, 2020)

5. BIBLIOGRAPHY

Attack.mitre.org. *Tactics - Mobile*. MITRE ATT&CK®. https://attack.mitre.org/tactics/mobile/

Attack.mitre.org. (2018). *Tactic TA0108 - ICS*. MITRE ATT&CK®. https://attack.mitre.org/tactics/TA0108/

Automated Collection, Technique T1119 – Enterprise. https://attack.mitre.org/techniques/T1119/

Allianz. (2016). *Cyber attacks on critical infrastructure*. Retrieved from https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

Antonio Aloisi, D. G. (2022, April). *The EU's Plan for improving Gig Economy*. Retrieved from https://www.adalovelaceinstitute.org/blog/eu-gig-economy/

Bank, E. C. (2020, October). *Report on a Digital Euro.* Retrieved from https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

BSI-Magazin. (2021, January). *Mit Sicherheit.* Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2021_01.pdf?__blob=publicationFile&v=4

Chermack, T. (2011). *Foundations of Scenario Planning: The Story of Pierre Wack (Routledge International Studies in Business History).* UK: Routledge.

Commission, E. (2022). *Regulatory framework proposal on artificial intelligence*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Detecon. (2022). *Online Education*. Retrieved from https://www.statista.com/outlook/dmo/eservices/online-education/eu-27

ENISA. (2016). *Threat Taxonomy.* Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy

ENISA. (2017, January). *Guidelines for SMEs on the security of personal data processing.* Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA. (2018). *Glossary of Terms.* Retrieved from https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

ENISA. (2018). *Looking into the crystal ball.* Retrieved from https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

ENISA. (2020, June). *A trusted and Cyber Secure Europe.* Retrieved from https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

ENISA. (2020, November). *Guidelines for Securing IOT.* Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ENISA. (2020). *Personal Data Breaches*. Retrieved from https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches

ENISA. (2020, March). *Raising Awareness of Cyber Security.* Retrieved from https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity/@@download/fullReport

ENISA. (2021). Retrieved from Foresight Challenges: https://www.enisa.europa.eu/publications/foresight-challenges

ENISA. (2021, July). *Understanding the increase in Supply Chain Security Attacks*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

ENISA. (2021). *Ad-Hoc Working Group on Foresight On Emerging And Future Cybersecurity Challenges*. Retrieved from https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group-on-emerging-and-future-cybersecurity-challenges

ENISA. (2021). *Threat Landscape.* Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA. (2022, July). *Cybersecurity Threat Landscape Methodology*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology/@@download/fullReport

ENISA. (2022). *Threat Landscape Report.* Retrieved from https://www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_de.pdf

ENISA. (n.d.). *Blockchain*. Retrieved from https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/blockchain

Erwin, S. (2022, March). *Cyber warfare gets real for satellite operators*. Retrieved from https://spacenews.com/cyber-warfare-gets-real-for-satellite-operators/

ESPAS. (2022). *THE MEGA-TRENDS*. Retrieved from https://ec.europa.eu/assets/epsc/pages/espas/chapter1.html

Fortinet. (2022). Retrieved from fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Forum, W. E. (2022, May). *Will the battle for space happen on the ground?* Retrieved from https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/

Fosnot, C. T. (1996). *Constructivism: Theory, Perspectives, and Practice.* Teachers' College Press.

Global, V. (2022, May). *44 Eye-Opening Gig Economy Statistics For 2022*. Retrieved from https://velocityglobal.com/blog/gig-economy-statistics/#:~:text=16%25%20of%20Americans%20have%20completed,via%20an%20

online%20gig%20platform.&text=Pew%20Research%20Center-,The%20number%20of%20global%20gig%20workers%20is%20expected%20to%20rise,to%2078%20mi

Harvey, F. (2018, June). *Are we running out of water?* Retrieved from https://www.theguardian.com/news/2018/jun/18/are-we-running-out-of-water

Hurst, A. (2022, April). *Cyber security skills gap contributing to 80% of breaches*. Retrieved from https://www.information-age.com/cyber-security-skills-gap-contributing-to-80-of-breaches-123499261/

IEA. (2017, November). *Digitalisation and Energy*. Retrieved from iea.org/reports/digitalisation-and-energy

Insights, F. B. (2022, June). *Everything as a Service*. Retrieved from https://www.fortunebusinessinsights.com/everything-as-a-service-xaas-market-102096

Institute, D. N. (2021). *Use Case: Designing Metrics to Measure Ecosystem Services.* Retrieved from https://nicholasinstitute.duke.edu/sites/default/files/escm/use-case-metrics-final.pdf

IPCC. (2022). *Climate Change 2022: Impacts, Adaptation and Vulnerability*. Retrieved from https://www.ipcc.ch/report/sixth-assessment-report-working-group-ii/

Johnson, B. D. (2011, April). *Science Fiction Prototyping: Designing the Future with Science Fiction.* Retrieved from https://www.morganclaypool.com/doi/abs/10.2200/S00336ED1V01Y201102CSL003

Jubb, S. (2022, August). *Escalating supply chain cyber-attacks need a strategic response*. Retrieved from https://www.openaccessgovernment.org/escalating-supply-chain-cyber-attacks-need-a-strategic-response/141371/#:~:text=What%20are%20supply%20chain%20attacks,and%20cause%20disruptions%20or%20outages.

Krajewski, R. (2021, January). *Why The Pandemic Led To An Increase In IT Outsourcing*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/01/28/why-the-pandemic-led-to-an-increase-in-it-outsourcing/?sh=5f530a102daa

Kymalainen, T. (2016, November). *Science Fiction Prototypes as a Method for Discussing Socio-Technical Issues within Emerging Technology Research and Foresight.* Retrieved from https://www.semanticscholar.org/paper/Science-Fiction-Prototypes-as-a-Method-for-Issues-Kymalainen/7d58c053b0b061b082e71b238b185a6d0b453861

M. Stojanovic, P. M. (2015). *THE SCENARIO METHOD IN URBAN PLANNING UDC 711.* Retrieved from https://www.semanticscholar.org/paper/THE-SCENARIO-METHOD-IN-URBAN-PLANNING-UDC-711-Stojanovic-Mitkovic/b9ca8565349bb41e188b1bb47c80fafce2c82221

Madiega, T. (2020, July). *Digital sovereignty for Europe.* Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Micro, T. (2019, July). *Cybercrime and Exploits: Attacks on Unpatched Systems*. Retrieved from https://www.trendmicro.com/vinfo/fr/security/news/vulnerabilities-and-exploits/cybercrime-and-exploits-attacks-on-unpatched-systems

Nations, U. (2022). *Population*. Retrieved from https://www.un.org/en/global-issues/population#:~:text=The%20world%20population%20is%20projected,and%2011.2%20billion%20by%202100.

Newman, L. H. (2021, December). *A Year After the SolarWinds Hack, Supply Chain Threats Still Loom*. Retrieved from https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/

Petrov, K. E. (2018, October). *Cybersecurity in Elections.* Retrieved from https://aceproject.org/ero-en/ifes-cybersecurity-in-elections

Platform, E. F. (2014). *European Foresight Platform*. Retrieved from http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/?msclkid=dafffcacc24311eca23e7f6fc4f3bd8f

Platform, E. F. (2014). *Megatrend / Trend / Driver / Issue*. Retrieved from http://foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/

Popova, N. S. (2017, September 7). The Importance of Megatrend Analysis. *Euromonitor International*. Retrieved from https://www.euromonitor.com/video/the-importance-of-megatrend-analysis#:%7E:text=A%20megatrend%20is%20a%20shift,new%20ideas%20disrupt%20entire%20industries

Qualitative Social Research. (2012). Retrieved from View of Uncovering Causality in Narratives of Collaboration: Actor-Network Theory and Event Structure Analysis: https://www.qualitative-research.net/index.php/fqs/article/view/1659/3281#:%7E:text=Event%20as%20a%20happening%20in,from%20one%20order%20to%20another

SAP. (2022). *Distributed energy resources (DER) and the rise of the prosumer*. Retrieved from https://www.sap.com/germany/insights/distributed-energy-resources-der-and-the-rise-of-the-prosumer.html

Schrage, M. (1999). Serious Play: How the World's Best Companies Simulate to Innovate . *Harvard Business Review Press.*

Shein, E. (2022, August). *Deepfake attacks and cyber extortion are creating mounting risks*. Retrieved from https://www.techrepublic.com/article/deepfake-attacks-and-cyber-extortion-are-creating-mounting-risks/

Shi, A. (2021, September). *Cyber Attacks Detection Based on Generative Adversarial Networks.* Retrieved from https://ieeexplore.ieee.org/document/9681469

Smart, E. (2021, November). *QUANTUM COMPUTERS WILL COMPROMISE THE SECURITY OF IDENTITY DOCUMENTS*. Retrieved from https://www.eurosmart.com/quantum-computers-will-compromise-the-security-of-identity-documents/

SOCRadar. (2022, May). *Common IoT Attacks that Compromise Security*. Retrieved from https://socradar.io/common-iot-attacks-that-compromise-security/#:~:text=Privilege%20escalation%3A%20Attackers%20could%20exploit,unauthorized%20access%20to%20the%20network.

Stackscale. (2021, April). *Internet traffic has rocketed globally from 2020 to 2021*. Retrieved from https://www.stackscale.com/blog/internet-traffic-globally-2020-2021/

Stiftung, B. (2022). *Trend toward authoritarian governance continues*. Retrieved from https://bti-project.org/en/reports/global-dashboard?&cb=00000

Stolton, S. (2020, October). *Europol charts 'value of accessing data' in encrypted cybercrime*. Retrieved from https://www.euractiv.com/section/digital/news/europol-charts-value-of-accessing-data-in-encrypted-cybercrime/

Taddeo, M. (2017, May). *Cyber Conflicts and Political Power in Information Societies.* Retrieved from https://www.researchgate.net/publication/317065626_Cyber_Conflicts_and_Political_Power_in_Information_Societies

TAMARA DENNING, B. F. (n.d.). *The Security Cards.* Retrieved from https://securitycards.cs.washington.edu/activities.html

Thomas Grisold, S. G. (2022, April). *The Five Diamond Method for Explorative Business ProcessManagement.* Retrieved from https://www.researchgate.net/publication/350948117_The_Five_Diamond_Method_for_Explorative_Business_Process_Management

Tim Starks, A. S. (2022, July). *Cyberattacks on satellites may only be getting more worrisome*. Retrieved from https://www.washingtonpost.com/politics/2022/07/29/cyberattacks-satellites-may-only-be-getting-more-worrisome/

Todd, D. (2021, February). *Future Attacks Against Cyber Connected Cars*. Retrieved from https://www.secureworld.io/industry-news/attacks-cyber-connected-cars

Union, E. (2022, May). *REPowerEU: A plan to rapidly reduce dependence on Russian fossil fuels and fast forward the green transition*. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3131

Wack, P. (. (2014). Scenarios: Uncharted Waters Ahead. *Harvard Business Review*. Retrieved from https://hbr.org/1985/09/scenarios-uncharted-waters-ahead. https://hbr.org/1985/09/scenarios-uncharted-waters-ahead

West, T. (2017). *The Future of Weaponized Artificial Intelligence*. Retrieved from https://threatcasting.asu.edu/sites/default/files/2019-12/ThreatcastingWest2017.pdf

TP-07-23-158-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
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-634-7
doi: 10.2824/117542