EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FORESIGHT CHALLENGES

A study to enable foresight on emerging and future cybersecurity challenges

NOVEMBER 2021

ABOUT ENISA

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

CONTACT

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

EDITORS

Rossella Mattioli, Apostolos Malatras, Marco Barros Lourenco, Eric Vetillard, Evangelos Rekleitis – ENISA and Volker Presse, Eve Naomi Hunter, Marco Gino Biasibetti Penso – Detecon

ACKNOWLEDGEMENTS

ENISA's Ad-Hoc Working Group on Foresight on Emerging and Future Cybersecurity Challenges

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-546-3 - DOI 10.2824/187824

TABLE OF CONTENTS

ABBREVIATIONS

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

PESTLE	Political, Economic, Social, Technological, Legal and Environmental dimensions (analysis method)
R&D	Research and Development
SWOT	Strengths, Weaknesses, Opportunities and Threats (analysis method)
STEEP	Sociological, Technological, Economic, Environmental and Political dimensions (analysis method)
TARA	Threat Agent Risk Assessment

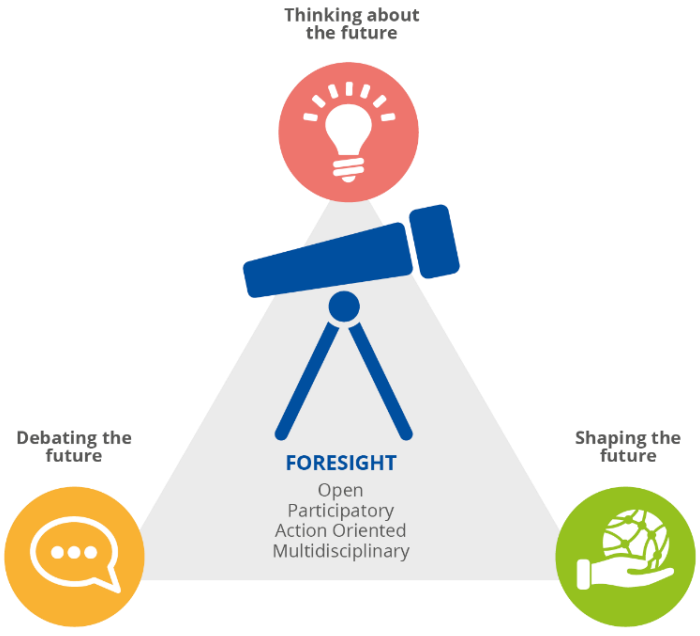
[1] https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

1. INTRODUCTION

Foresight[2] **is a complex, multi-stage, ideally ongoing process, the ultimate aim of which is informed decision-making with regard to securing strategic plans for possibly diverse future developments.** It enables reflection on various possible futures and strategic preparation for plausible scenarios.**[3]** Since the mid-1950s and early 1960s, foresight as a discipline has grown to become a major strategic planning tool for private corporations as well as the public sector.[4] .

Foresight is still evolving and changing today. That is largely because it is **action-oriented**, and therefore has tangible results; it is **open**, meaning there is freedom within foresight to think outside of the box or to reshape previous notions; lastly it is **participatory and multidisciplinary** – foresight brings together diverse groups that have expertise in a wide range of topics, thus providing more realistic and thoughtful possible futures.[5]

Figure 1: Foresight Overview[6]



Source: JRC-IPTS (modified)

"Foresight is neither prophecy nor prediction. It does not aim to predict the future – to unveil it as if it were predetermined – but to help us build it." – EU Foresight Platform[7]

[2] Please note that foresight is often referred to as "strategic foresight" and "futures studies."

[3] See GCPSE, Foresight – The Manual, UNDP Global Centre for Public Service Excellence, Singapore, 2014.

[4] Schwartz, P. (2012). The art of the long view: planning for the future in an uncertain world.

[5] European Foresight Platform (efp), What is Foresight?, 2010, http://www.foresight-platform.eu/community/forlearn/what-is-foresight/.

[6] The Institute for Prospective Technological Studies (IPTS) is one of the seven scientific institutes of the European Commission's Joint Research Centre (JRC). This image from JRC-IPTS, European Foresight Platform is available here: http://www.foresight-platform.eu/community/forlearn/what-is-foresight/ and has been adapted for the purposes of this study.

[7] European Foresight Platform (efp), What is Foresight?, 2010, http://www.foresight-platform.eu/community/forlearn/what-is-foresight/

There are three main benefits[8] of foresight:

- knowledge generation,
- facilitation of stakeholder relationships,
- capability enhancement.

Knowledge helps individual stakeholders best position themselves for future developments; with knowledge, they can see beyond the fallacy that the future will look much like the present and imagine leading-edge futures (Wilkinson, 2013). The process of developing this knowledge and insight **increases connections between stakeholders**, thus strengthening related networks – in this case the cybersecurity community. Finally, foresight can **contribute to capability enhancement,** during which organizational and stakeholder capabilities may be prioritized based on the findings of the foresight activity. This information is critical for identifying and enabling the development and acquisition of key skills, policies, and technologies.

The application of foresight in the field of cybersecurity is not currently widespread.[9] However, we strongly believe that embedding these methods into the cybersecurity industry will lead to an even more nuanced, clear, and multidisciplinary understanding of risk, as well as the strategic ramifications of security measures.

Foresight is already a key element of ENISA's strategy; it increases knowledge and understanding of emerging and future challenges, thus providing a path to find solutions that address those challenges and bolster EU resilience to cybersecurity threats.[10]

As an additional resource for integrating foresight into the field of cybersecurity, this report provides an overview of key aspects of foresight, a selection of key methods and tools, best practices for applying foresight, and finally, an exemplary guide to putting this knowledge into practice, and running a foresight activity. We provide recommendations tailored specifically to ENISA's wide range of functional needs – executive strategy, policy support, capacity building, operational cooperation, and certification activities. As these functional needs are likely shared by many readers of this report, the recommendations are formulated as to be easily adapted to fit other organizations and contexts.

With this initiative we hope to inspire and support Member States and other partners to use foresight to address their own cybersecurity challenges. ENISA is taking the first step by beginning to use these methods internally to provide more accurate and prescient information to our stakeholders.

1.1 OBJECTIVES AND SCOPE

To adequately address future cybersecurity threats and to shape a more secure society, ENISA aims to draw upon findings and research from the futures and foresight community to develop a process to apply foresight to cybersecurity. By fostering the ability to understand potential futures, ENISA will be able to better shape both itself and the European cybersecurity ecosystem to address and manage emerging and future challenges.

This project aims to deliver an exemplary structured foresight framework (comprised of a selected set of foresight methods applied to representative use cases) for generating trend

[8] Haegeman, K., Spiesberger, M., Könnölä, T., Evaluating foresight in transitional research programming, Technological Forecasting and Social Change 115, 2017, pp. 313 – 326.

[9] Althonayan, Abraham, and Alina Andronache. "Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment." 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). IEEE, 2019.

[10] See ENISA's strategy here: https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

outlooks, scenarios and perspectives on the future to help ENISA to identify and address emerging and future cybersecurity challenges.

The framework or sets of methods recommended must be suitable for the range of ENISA activities including strategic long-term planning, research agenda setting, threat landscape evaluation, and formation of future policy priorities. It is therefore required that the framework be flexible and easily adapted to each context and environment.

This report is not intended to be a comprehensive overview of all foresight methods available, but rather aims to highlight the most relevant methods – based on ubiquity or suitability to ENISA's core foresight needs.

1.2 TARGET AUDIENCE

This report is targeted at stakeholders within the cybersecurity community (specifically ENISA internal and external stakeholders) but can very well be applied more broadly, as foresight methods are generally applicable across industries or topics. This report may be especially relevant for:

- Policymakers and national authorities with cybersecurity responsibilities
- ENISA stakeholders, decision- and policymakers in the areas of ENISA's portfolio
- Cybersecurity researchers, practitioners, and educators
- Relevant experts within European Institutions, Bodies and Agencies and their partners
- Futurists or foresight consultants
- Organizational leaders and corporate strategists
- Forecasters and prediction market developers

1.3 STRUCTURE OF THE REPORT

The report reflects the progression and outcomes of the research study and is structured as follows.

Figure 2: Structure of Report

Chapter 2 // Stocktaking: This chapter describes the research methods used to create this report – a literature review and stakeholder interviews.

Chapter 3 // Foresight Methods & Frameworks: The methods collected in the stocktaking phase of the study are narrowed down. We categorize and define a selection of useful methods to grant the reader familiarity with foresight, its purposes and possible application contexts.

Chapter 4 // Selection Criteria: To narrow down the plethora of methods available, we define selection criteria and organize identified methods according to key selection criteria.

Chapter 5 // Best Practices: Practical advice and recommendations gleaned from the stocktaking phase are presented in this chapter.

Chapter 6 // Application Use Cases: ENISA's primary use cases for foresight are defined in this chapter. For each use case, we propose an appropriate framework of methods, tools, processes, and formats.

2. STOCKTAKING

2.1 OVERVIEW

To develop this framework, ENISA conducted a thorough literature review to explore a broad range of information on foresight, with a focus on methods, tools and applications that could be relevant for ENISA.[11]

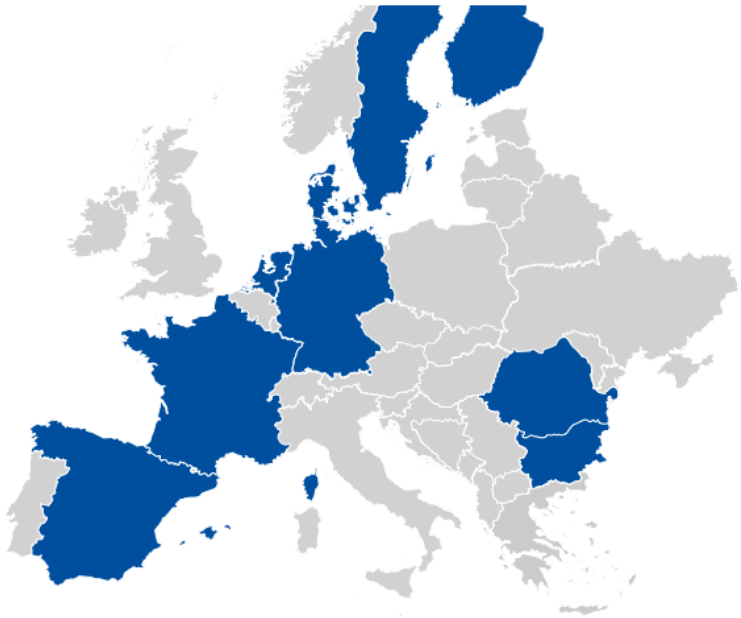
These findings were augmented by interviews with experts in the fields of foresight and cybersecurity, members of the ENISA's Ad-Hoc Working Group on Foresight on Emerging and Future Cybersecurity Challenges.[12] The output of the research phase was the collection of definitions, key characteristics, and best practices for a select representative set of methods (relevant to ENISA's specific operating environment).

2.2 STAKEHOLDER ANALYSIS

Experts interviewed for this project were primarily individuals in ENISA's Ad-Hoc Working Group on Foresight (one additional academic foresight expert and practitioner was interviewed). All experts brought unique perspectives that shed light on the characteristics of various foresight methods and best practices for planning and conducting foresight exercises.

The experts interviewed as a part of this project represent a diverse group of individuals. We interviewed 16 people, who represent (in nationality) nine different Member States, geographically distributed across the EU. The expert group consisted of approximately 60% women and 40% men.

Figure 3: Geographical Distribution of Experts

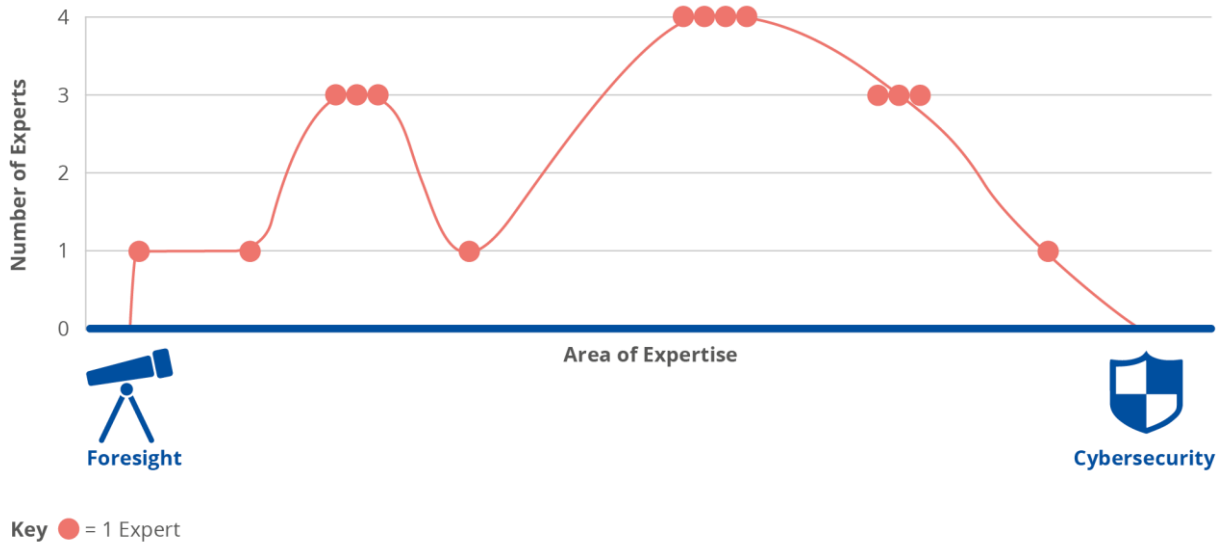


[11] Due to the practical application of the recommendations in this report, our research focused primarily on frameworks, methods, and tools and did not target the breadth of the foresight literature that focuses on principles, ethics, attitudes, learning factors, and other more intangible factors.

[12] See https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group-on-emerging-and-future-cybersecurity-challenges

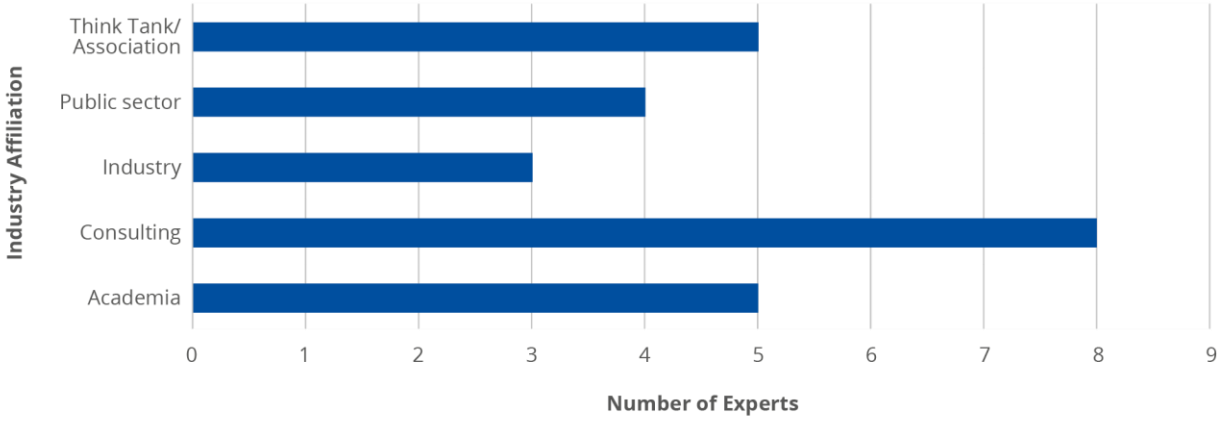
The expert group also contains a mixture of foresight experts and cybersecurity experts. The graph below illustrates how experts rated themselves on a slide scale when asked: “Does your expertise lie more in cybersecurity or foresight?”

Figure 4: Expert Group Areas of Expertise



The experts work within a wide range of industries, but primarily in academia and consulting.

Figure 5: Expert Industry Affiliation



3. METHODS AND FRAMEWORKS APPLICABLE TO FORESIGHT FOR CYBERSECURITY

3.1 INTRODUCTION

Each foresight activity begins with the identification of scope, objectives, and stakeholders – this step is a critical success factor. The scoping and initiation process is described in more detail in later sections of the report.

Depending on the aim of the foresight project, (and factors such as the point in time to be analysed (time horizon), field of application, scope of the project, available resources (human, time, financial), ability to shape future evolutions), a specific set of methods is selected to best fit the specified project.

A foresight exercise requires **thoughtful preparation, involvement of the stakeholders and participants, constant monitoring, skilful management, and continuous adaptation**. This chapter categorizes methods based on their "intention," future-handling approach, and overall aim.

For a comprehensive description of the entire foresight process and overview of foresight methods, we refer the interested reader to the European Foresight Platform,[13] a very useful resource and reference.

Foresight Intentions[14]

Foresight activities usually involve three mutually dependent and essential intentions: diagnosis, prognosis, and prescription. Foresight activities usually include all three of these intentions at different points in the project.

This categorization helps to better identify the goal of each use of a method and supports the method selection process. It was created by the EU Foresight Platform.[15]

[13] "The European Foresight Platform is a global network building program supported by the European Commission. It aims at building a global network that brings together different communities and individual professionals to share their knowledge about foresight, forecasting and other methods of future studies." – EFP http://www.foresight-platform.eu/

[14] "Intention" is not a word used in the foresight industry, it is rather used in this report to distinguish between lower-level objectives within a project and the primary objectives and desired outcomes.

[15] http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/process/methodology/Smith

Table 1: Foresight Intentions

Foresight Intention	Description
Diagnosis	The aim is to evaluate the current context or state of affairs or subject of study, to recognize early signs of possible future changes.
Prognosis	The aim is to create or envision probable, possible and plausible future states of a subject of study.
Prescription	This component involves participants inventing possible strategies, roadmaps or policies that aim to either respond to possible futures, or actively shape the future towards a desired direction.

Future Handling

Based on the primary objectives of the foresight activity, the project or method's approach can be either **"responsive", meaning to devise strategies to react to possible events, or "normative", to design a future (that can be desirable or undesirable)** and then take steps to impact that chosen future. This topic is a subcategorization of the prescriptive intention.

3.2 OVERVIEW OF SELECTED METHODS AND FRAMEWORKS

Both cybersecurity and foresight benefit from a diverse and interdisciplinary environment. For this reason, it is often wise to integrate frameworks from other fields. We believe that the guidelines, practices, approaches, methods and tools of both **systems thinking** and **user-centred design** can be key to establishing the right mindset when approaching foresighting in the field of cybersecurity.

User-centred design offers a set of guidelines and tools that focus on the human factor in business and technological implementations, helping to better define and design interactive systems and organizations [16]. The framework makes extensive use of immersive analysis and empathy exercises, providing a window into the thoughts, aspirations, desires, needs and actions of the human actors.

The framework of systems thinking, on the other hand, allows us to "see the forest through the trees."[17] [82] This phrase distils the essence and objective of the framework: to enable its practitioners to identify, observe, analyse and shape systems, as well as the relationship dynamics between its elements.

Both frameworks may provide a foundational aspect of a foresight project and support the development of a point of view or mindset. Because the scope of these frameworks is so broad, we have not included them in the categorizations in section 3.2.1, nor going forward in this report. Nevertheless, they remain highly relevant aspects for any foresight practitioner seeking to implement the tools, methods and processes outlined in this report.

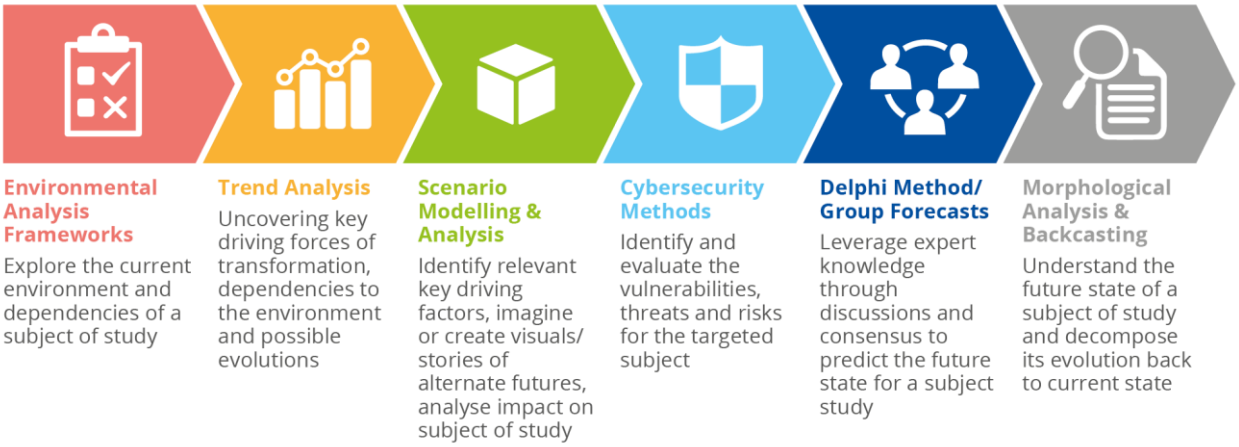
[16] https://www.interaction-design.org/literature/topics/user-centered-design
[17] Senge, Peter M. (1990). The fifth discipline: the art and practice of the learning organization. New York: Doubleday/Currency,

3.2.1 Method Categorisation

To better illustrate the range of methods, the relevant methods, frameworks, and tools have been grouped into six categories driven by the stocktaking phase of this project.[18] Not all methods listed can be considered explicit to foresight – we have also included strategic planning methods and problem-solving techniques that are often integrated into foresight activities.

Likewise, cybersecurity analysis methods are also included here to provide an overview of relevant approaches for foresight in cybersecurity. These methods and techniques are not used in traditional foresight but may be applied if they support the objectives of the foresight activity. For that reason, a selection of methods is included in this report for future reference.

Figure 6: Selection of methods used in foresight[19]



3.2.2 Environmental Scanning / Analysis Frameworks

Environmental analysis frameworks enable the user to systematically explore a chosen environment,[20] with the goal of detecting weak signals[21] of incoming change that could significantly impact the future. These methods provide a structured and analytical view of the current situation in order to create common understanding. This category of methods usually draws upon the diagnostic intention.

There are different techniques to scan the environment including, for example:

- **STEEP** – framework to analyse Socio-cultural, Technological, Economic, Environmental and Political factors of a particular arena.
- **PESTLE** – framework to analyse Political, Economic, Socio-cultural, Technological, Legal and Environmental factors of a particular arena.
- **SWOT** – framework to identify and analyse the Strengths, Weaknesses, Opportunities, and Threats for a particular topic or entity.

[18] For other ways of categorising methods, see: Jack & Saritas, Ozcan. (2011). Science and technology foresight baker's dozen: A pocket primer of comparative and combined foresight methods. foresight. 13. 79-96.

[19] The methods used in foresight are difficult to classify into mutually exclusive categories. The categories oftentimes overlap content-wise and tend to be divided differently in various publications.

[20] Here "environment" refers to circumstances and context - not an ecological environment.

[21] Weak signals are the initial indications of a significant trend or change.

Each of the above frameworks enables the systematic evaluation of the characteristics, developments, and influences in the listed domains to get an understanding of the environment. There are also other variations of these frameworks that take other domains into account – the choice of method or domain should be based on an initial analysis of the given subject.

3.2.3 Trend Analysis

A trend is defined as a tendency of a development over time, or an emerging pattern of change that commonly influences large social groups.[22] Trend analysis methods usually serve prognostic or diagnostic intentions.

Trends can be analysed in many ways – for instance, by means of literature reviews, bibliometrics, text-mining, patent analyses, and trend impact analyses, among others. These methods identify current or emerging trends and typically explore the cause, potential impact, probability, and speed of occurrence of those trends.[23]

Further methods used to analyse trends include:

- **Causal Layered Analysis** – Supports the identification of driving forces by gaining insight into participants' perceptions such as world views, values, and cultural norms
- **Trend Radars** – provides a cross-industry view of emerging and already existing trends within the target environment
- **Trend Impact Analysis** – analysis of the impact of one or more possible events on the extrapolation of a trend into the future.
- **Horizon Scanning** – Systematic monitoring of current trends as well as the identification of new, relevant developments in a particular area through a creative process of collective sense-making.

3.2.4 Expert Group Foresight

Expert group foresight covers a variety of methods, where a group (or a crowd) of participants provides input on the issue under study. The best-known members of the expert group foresight family are the Delphi method and expert panels. In both, experts share their insights about the future. The Delphi method however involves a more structured communication method to elicit answers from experts. Experts are usually involved to support a foresight project with its prognostic or prescriptive intentions.

Delphi is an explorative method based on a structured and iterative group communication between subject matter experts expressing judgements on the chosen topic. In the first sequence, various experts in a particular field are surveyed separately about a specific topic or question. Afterwards, their anonymized contributions are collected, and experts are asked to provide feedback to the collected insights. To reach a consensus, this process would be repeated multiple times. This approach helps to avoid groupthink and therefore tends to generate more creative ideas from a variety of perspectives. The entire process can be conducted remotely, which makes it easier to engage a more diverse expert group from all over the world. This method can be time-consuming, especially when there are multiple iterations. Japan's National Institute of Science and Technology Policy (NISTEP) conducts foresight exercises approximately every five years, most of which rely on a large Delphi study with approximately 2000 participants.[24]

[22] See efp, Megatrend / Trend / Driver / Issue, 2010, http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/megatrend-trend-driver-issue/

[23] See GCPSE, Foresight – The Manual, UNDP Global Centre for Public Service Excellence, Singapore, 2014.

[24] Please see https://www.nistep.go.jp/en/?page_id=56

Other examples of expert group-based methods include:

- **Aggregated Judgements / Group-based Forecast** – logically combines multiple individual judgements into consistent and collective judgements.
- **Key Technology Study (Technology Forecasting)** – applies sets of criteria to critical technological developments in order to enable informed assessments

Note that there are also crowd or participatory foresight methods, in which inputs are solicited from non-experts.

3.2.5 Scenario Methods

Scenario methods are some of the most used and well-known **prognostic** methods in foresight. They are used as exploratory tools to think about possible, desired or undesired futures rather than to predict a single future in detail. These methods can also be used to simulate and test various solutions prior to determining an optimal strategy. Usually, more than one possible future is explored to support decision-making that avoids potential challenges and pitfalls.

Scenario generation is typically preceded by a diagnostic phase that allows for the informed consideration of key factors that can impact the future of the issue at hand. Thinking about multiple possible futures raises awareness of various factors that may affect the future; this knowledge enables the development of more flexible, future-proof, adaptive strategies.

Scenarios can be approached with various methods, for example:

- **Gaming** – devising games or roleplay scenarios to test possible strategies or solutions by identifying possible reactions to and consequences of their implementation.
- **Visioning** – looking to the ideal future to create a strategy to achieve specific goals.
- **Cross Impact Analysis** – evaluates the likelihood of specific future events occurring by assessing probability of other events occurring and then exploring their mutual relationship.

3.2.6 Morphological Analysis and Backcasting

This category covers methods that are not typically associated but share the same two characteristics - a prescriptive foresight intention and focus on event regression and system decomposition. Regression analysis in foresight follows a similar approach to statistical regression analysis. However, regression analysis in foresight works with qualitative data and subjective opinion, as opposed to quantitative methods to identify events and event triggers that may lead to a predicted future event.[25] Decomposition, on the other hand, seeks to break down complex systems into smaller parts to facilitate analysis of its components, the dynamics governing the interaction of components and the effect they have on the system.

Morphological Analysis is a creative, heuristic, normative method that supports the exploration of complex problems and possible solutions using a multi-dimensional matrix. It is a time-consuming group exercise that requires facilitation.[26]

Backcasting is another normative method that centres a selected scenario of a desirable (or undesirable) future. The participants then move backwards in time to identify the decisions or events that need to take place to transform that selected scenario into reality. Through

[25] https://hbr.org/2015/11/a-refresher-on-regression-analysis
[26] Jackson, M., Practical Foresight Guide, 2013.

backcasting, organizations can plan which actions they should take and evaluate potential consequences. It raises awareness of the fact that the future is determined by many factors and that different actions lead to various alternative outcomes.[27]

Threatcasting is a multi-stage method that involves envisioning an unwanted future, then reconstructing steps and decisions that need to be taken to prevent that future from occurring. It was designed primarily for analysing military futures. Threatcasting combines many foresight methods including Delphi, science fiction prototyping, backcasting, and scenario modelling. This method has a defined time horizon – each activity is designed to look forward 10 years into the future.[28]

Other methods included in this category are:

- **Technology Sequence Analysis** – generates probable timelines for technology releases by analysing estimates of the time required for intermediate technical steps
- **Roadmapping** – produces a document that defines the steps and milestones necessary to obtain a desired future
- **Multi-criteria Analysis** – compares possible identified solutions against a weighted set of assessment criteria.
- **Synectics** – promotes new and creative ways of thinking by, for example, imagining a chosen problem in an unusual, unconnected environment

3.2.7 Cybersecurity Analysis Methods

As a discipline, cybersecurity often assesses risk and potential future threats, incidents and crisis scenarios. These methods are all variations of risk assessment techniques. Each is slightly different in terms of focus (e.g., on the threat actor or on visualization) but all aim towards identifying and prioritizing risk and subsequently responding to that risk. The methods in this category can be used for diagnosis, prognosis, or prescription.

Below are a few well-established methods for risk analysis and threat modelling.

- **Threat Agent Risk Assessment (TARA)**[29] – a threat-based risk assessment method used to identify, assess, and prioritise risks. It takes threat actors, their motivations, and possible methods into account.
- **Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)**[30] – a comprehensive evaluation method to identify, rank, and manage cybersecurity risks.
- **Threat Modelling**[31] – a conceptual analysis technique used for identifying potential vulnerabilities and developing measures in the early stages of application or service development. There are many frameworks and methods for threat modelling,[32] one such method is **Attack Trees**.[33] Attack Trees support the formulation of trees of possible techniques that may help an attacker achieve their objectives.

[27] Jackson, M., Practical Foresight Guide, 2013.

[28] Vanatta, N., Johnson, B. D., Threatcasting: a framework and process to model future operating environments, SAGE, 2019, pp. 79 – 88.

[29] See Rosenquist, M., Prioritizing Information Security Risks with Threat Agent Risk Assessment, Intel Information Technology, USA, 2009.

[30] See https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473. Note that Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

[31] See Barber, C., *Cyber Security Predicting the Future, 2020.*

[32] See https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

[33] The Attack Trees was created by cybersecurity researcher Bruce Schneier. For more information see his description here: https://www.schneier.com/academic/archives/1999/12/attack_trees.html or refer to Saini, V., Duan, Q., Paruchuri, V., *Threat modelling using attack trees,* 2008.

4. SELECTION CRITERIA

The first step of any foresight activity is scoping; during this phase the person or group responsible for the activity defines key objectives and reviews the context of the activity. Once completed, they may consider the following key criteria to narrow down the choice of foresight methods, tools, and/or frameworks.

- **Target outcomes and deliverables –** which methods, tools, and/or frameworks will most likely produce the required effects on stakeholders? Which will most likely produce the deliverables expected from the foresight activity?
- **Foresight intention –** Consider the foresight intentions described in 3.1 for each step of the planned activity. Is the objective to diagnose a current state, or to prognose or prescribe a future state? The selection of methods must be based on suitability to the underlying objectives of the foresight activity.
- **Future handling approach –** Should your activity be more responsive or normative? Is the objective to prepare to respond to events or shape futures?
- **Time horizon –** The time horizon is the point in the future that targeted by the foresight activity. Which methods, tools, and/or frameworks can be implemented to diagnose or prognose events, or prescribe handling options, for the fixed point in time which will be evaluated during the activity?
- **Activity timeframe –** Which methods can be completed within the timeline set for the execution of the foresight activity? Are there tools or frameworks that could support the on-track and timely execution of the activity?
- **Required resources/skills –** What access does the project have to administrative support, data available on the subject, expert participants, financial resources, etc.?

Multiple experts emphasized that the choice of method highly depends on the context of the exercise, including the following more abstract criteria:

- **Clarity of desired outcomes –** Any ambiguity towards desired outcomes must be clearly addressed before method selection. The methods that are applied must help produce outcomes that are useful and usable for the project's key stakeholders.
- **Participant Group –** All methods must consider the unique characteristics of the participant group; they should enable maximum engagement, capacity for creative thinking, and transparent communication. If the participants are already known to the organizer, key factors to analyse include existing or expected group dynamics, personalities, roles, and areas of interest.
- **Publicity –** If one goal of the foresight activity is to generate publicity, scenario modelling techniques are usually favoured because they are the most attention-grabbing and easiest to describe. However, the findings of the activity may be misrepresented by the press, which may undermine the diplomatic process or other relationships with stakeholders. These facets should be evaluated for each foresight activity.

- **Experience –** Experts from the Working Group stated that when they use methods they are familiar with (as opposed to methods unfamiliar to them), the activities progress more smoothly and tend to generate more dynamism and interaction. Nonetheless, the benefits that the facilitator may gain from familiarity should be secondary to selecting methods that support the objectives of the exercise.

4.1 FORESIGHT METHOD COMPARISON

The following table presents a selection of methods, along with their selection criteria and core characteristics. The selection includes methods that are either commonly used, innovative, and/or especially useful to address ENISA's foresight needs. In this table, we have categorized methods by the overarching categories described in the previous chapter, the foresight "intention" that the method would support, and a categorization of each method's usual future-handling approach (responsive or normative). Other factors included in the table are estimated time needed for each method, special resources required, and overall aim of the method.

Table 2: Methods Analysis

Category	Method	Underlying Objective of Activity			Time-horizon covered			Future-handling approach		Estimated time needed for method	Special resources required	Aim
		Diagnostic	Prognostic	Prescriptive	Short-Term	Mid-Term	Long-Term	Responsive	Normative			
Scenario Modelling & Analysis	**Scenario Methods**[34]		v	v	v	v	v	v	v		Professional facilitator; presence of decision makers; the means to make use of the strategic direction drawn from the study.	To enrich strategic decisions by simulating and analysing possible futures. Thinking beyond the boundaries of "business as usual".
	Visioning[35]		v		v	v	v		v	From days to months; time consuming		To create a common vision of the desired future while taking into account the current point of departure before the decision-making stage
	Gaming[36]		v	v	v	v	v	v	v	1-6 months	Stakeholders; representatives	To simulate various scenarios or solutions to gain a better understanding of operational dynamics and perspectives.
	Cross-Impact analysis[37]		v		v	v	v			At least 2-8 months	Multidisciplinary group of experts; supporting software	To understand how one future event might alter probability of other events happening
	Bipolar Factors		v		v	v	v		v	Less than 1 week	Key driving forces or scenario topics	Use combinatorial procedures to enable the creation of multiple alternate scenarios based on various key driving factors or topics.
Trend Analysis	**Trend Watching/ Cool Hunting**		v		v	v	v					To identify emerging trends and predict which trends will be perceived as "cool".
	Wild Cards and Weak Signals[38]		v									To identify possible emerging trends or explore unexpected events that can change the course of the future.
	Trend Radars		v		v	v	v					To assess emerging trends and their relevance to a specific issue based on selected criteria.

[34] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/scenario/
[35] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/creative-methods/visioning/
[36] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/creative-methods/gaming/
[37] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/cross-impact-analysis/
[38] See GCPSE, Foresight – The Manual, UNDP Global Centre for Public Service Excellence, Singapore, 2014.

Category	Method	Underlying Objective of Activity			Time-horizon covered			Future-handling approach		Estimated time needed for method	Special resources required	Aim
		Diagnostic	Prognostic	Prescriptive	Short-Term	Mid-Term	Long-Term	Responsive	Normative			
	Trend Interpolation and Extrapolation[39]		v		v						Historical data	To project a trend into the future based on historical data on the rates of change. Less reliable for mid- and long-term time horizons.
	Trend impact analysis[40]		v		v	v					Historical data	To envision future impact based on quantitative extrapolation of historical data; consider potential events that could modify the original extrapolations.
	Patent analysis[41]	v	v		v	v	v					To identify possible technological trends by exploring recently patented technologies.
	Modelling & Simulation[42]		v	v	v	v	v				Access to knowledgeable researchers and software developers + modelling software.	To gain insight into possible future developments by experimenting with computer models that simulate real-world processes, e.g., test resources needed to improve system performance.
	Causal Layered Analysis (CLA)[43]	v			v	v	v				Expert facilitators	To discover various perspectives; to understand how different stakeholders interpret issues, to identify whose voices are being heard or not; to discover different ways of knowing/learning
Delphi Method / Group Forecasts	**Delphi Study[44]**	v	v	v			v	v	v		Access to experts who will commit to longer term participation.	To create consensus on a topic based on an anonymous expert survey in at least 2 rounds, where experts make judgements, and provide feedback on each other's assessments
	Aggregated or group-based judgements		v		v	v	v					To formulate a collective set of judgements by aggregating the set of individual judgements (by experts or non-experts, depending on context).

[39] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/trend-intra-extrapolation/
[40] See Jackson, M., Practical Foresight Guide, 2013.
[41] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/patent-analysis/
[42] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/gaming-simulation-and-models/modelling-simulation/
[43] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/creative-methods/causal-layered-analysis-cla/
[44] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/classical-delphi/

Category	Method	Underlying Objective of Activity			Time-horizon covered			Future-handling approach		Estimated time needed for method	Special resources required	Aim
		Diagnostic	Prognostic	Prescriptive	Short-Term	Mid-Term	Long-Term	Responsive	Normative			
	Expert Panel[45]		v	v		v	v	v	v	3-18 months	A composition of 12-20 experts to cover the knowledge required	To elicit expert judgement on a future of a given topic, while allowing for networking between different disciplines, followed by creation of report where priorities are set.
	Key Technology Study[46]		v		v	v						Method of technology forecasting to gain informed assessment on critical technological developments.
Environmental Analysis Frameworks	**Environmental scanning**[47]	v			v	v	v			Ideally an ongoing process	Access to information sources; skilled consultants or expert panel	To detect weak signals of important future changes and summarize important characteristics of the present
	Horizon scanning[48]	v	v		v	v	v				Information sources	To identify emerging issues or events that might become threats or opportunities
	Bibliometrics, text-mining, literature review[49]	v	v		v	v	v					To identify possible (technological) changes based on researching texts / literature / publications.
	Structural analysis[50]	v								At least 6 months	10 experts + 2-3 person technical committee; supporting software e.g. MICMAC or MACTOR	To identify the key/driving variables within the system and how they impact or are dependent on the others
	SWOT analysis[51]	v			v	v	v					To systematically identify major issues to consider during strategic decision-making (strengths, weaknesses, opportunities, threats.)

[45] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/expert-panels/
[46] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/expert-panels/key-technology-study/
[47] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/environmental-scanning/
[48] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/horizon-scanning/
[49] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/bibliometrics/
[50] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/structural-analysis/
[51] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/swot-analysis/

Category	Method	Underlying Objective of Activity			Time-horizon covered			Future-handling approach		Estimated time needed for method	Special resources required	Aim
		Diagnostic	Prognostic	Prescriptive	Short-Term	Mid-Term	Long-Term	Responsive	Normative			
	STEEP[52]	v			v	v	v					To gain a comprehensive understanding of the social, technological, economic, environmental, and political factors affecting a particular issue.
	PESTLE[53]	v			v	v	v					To gain a comprehensive understanding of the political, economic, sociological, technological, legal, and environmental factors affecting a particular issue.
Morphological Analysis & Backcasting	**Technology Sequence Analysis**[54]		v			v	v					To forecast a duration of time after which specific technology-dependent systems might become available.
	Morphological Analysis[55] **and Relevance trees**			v	v	v	v		v		Availability of directly concerned stakeholders	To examine all possible paths to an objective and choose the optimal one
	Roadmapping[56]			v	v	v	v	v	v		Participation of key experts	To develop, organize, and present information on critical milestones that must be achieved to make a desired future a reality.
	Backcasting[57]			v			v		v	1-2 years	Stakeholder involvement; Financial means to implement action plan.	To develop normative scenarios and gain a deeper understanding of their feasibility and implications by testing alternative solutions.
	Multi-criteria analysis[58]			v	v	v	v	v	v		Expert or group of decisionmakers; supporting software	To compare various solutions along a set of weighted criteria

[52] See GCPSE, Foresight – The Manual, UNDP Global Centre for Public Service Excellence, Singapore, 2014.
[53] See https://rapidbi.com/the-pestle-analysis-tool/
[54] See Jackson, M., Practical Foresight Guide, 2013.
[55] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/morphological-analysis/
[56] See Jackson, M., Practical Foresight Guide, 2013.
[57] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/roadmap/backcasting/
[58] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/analysis/multi-criteria-analysis/

Category	Method	Underlying Objective of Activity			Time-horizon covered			Future-handling approach		Estimated time needed for method	Special resources required	Aim
		Diagnostic	Prognostic	Prescriptive	Short-Term	Mid-Term	Long-Term	Responsive	Normative			
	Synectics[59]			v	v	v	v	v	v			To find innovative solutions to a problem by generating analogies and fitting the new solutions to the original problem.
	Threatcasting[60]			v			v		v		A diverse group of subject matter experts	To develop normative scenarios that will allow the group create strategies to avoid, mitigate or recover from threats.
Cybersecurity Analysis Methods	**TARA**[61]	v			v	v	v	v			Knowledge of threat actors and attack methods	To identify areas of exposure based on threat agent motivations and likely methods of attack
	OCTAVE[62]	v	v	v	v	v		v			Overview of assets and requirements	To assess and manage risk to an organization by holistically reviewing organizational requirements and priorities.
	Threat modelling[63]		v		v	v		v			Knowledge of attack methods	Graphically illustrate the ways in which an attacker may reach their goal (e.g., gain access to financial records).

[59] See http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/methods/creative-methods/synectics/

[60] See Vanatta, N., Johnson, B. D., Threatcasting: a framework and process to model future operating environments, SAGE, 2019, pp. 79 – 88.

[61] See Rosenquist, M., Prioritizing Information Security Risks with Threat Agent Risk Assessment, Intel Information Technology, USA, 2009. https://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

[62] For more information on Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), see https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473

[63] See Barber, C., *Cyber Security Predicting the Future, 2020.*

4.2 TOOLS

Not quite at the level of a method, tools are supporting frameworks or platforms that aid the application of foresight methods. This section provides a non-exhaustive overview of the types of tools available. While some are efforts to "digitalise" foresight, others simply enhance the in-person foresight experience. When selecting tools for a specific foresight activity, we recommend reviewing other possible sources as there are some tools designed for a specific audience or context.

Workshop Facilitation Tools

These tools and techniques are often used by workshop facilitators to ease communication in workshops or to elicit creative ideas from participants. Some well-known examples are:

- **Brainstorming**, where participants are encouraged to generate large amount of raw, spontaneous ideas, while getting inspired by the ideas of other participants, without being subjected to immediate judgement.
- **World Café**, where a large group of participants can discuss various questions in a structured way, in rounds, within smaller groups, and note down their ideas on large sheet of paper for the remaining groups to see and serve as reference.
- **Mind mapping**, a technique of graphic facilitation to help visually organize collected information.

There are now a few digital databases that provide information on foresight-relevant tools. One source for identifying additional foresight-relevant tools is the website Service Design Tools[64] which describes and organizes tools based on the stage of the design process, stakeholders and participants, the aim of the activity, and desired visualization methods. Other resources include the Futures Platform,[65] the Governance Futures Toolkit,[66] and Teach the Future[67] (which aims to provide educators tools to integrate foresight into their curricula.)

Artificial Intelligence (AI)-Based Tools

AI-based tools may assist foresight activities like assessment of the current environment, trend analysis, or trend extrapolation. While not ubiquitous, these tools are now often integrated into the foresight process.[68] AI software can be especially helpful for text-mining and analysing large datasets, for instance to identify terms and phrases possibly indicative of emerging or future trends or to support a literature review. Natural Language Processing is typically used for these activities. AI-based tools may also support the selection of scenarios.

Collaboration Tools & Foresight / Trend Databases

To better facilitate foresight exercises, many experts recommend the use of collaboration tools (such as digital whiteboards and note-taking apps), as well as research databases for desktop research and trend recognition. It is important to note that within the expert community existing radar databases and foresight information sources are not always trusted. These sources rarely publish details on the information gathering and preparation process, therefore the experts interviewed typically rely on their own research or primary sources to determine trend-related information.

[64] POLI.design and Oblo, Service Design Tools, Tools, https://servicedesigntools.org/tools
[65] https://www.futuresplatform.com/product
[66] https://www.iftf.org/uploads/media/GovFuturesLab_Toolkit.pdf
[67] https://www.teachthefuture.org/
[68] Kayser, Victoria, and Knut Blind. "Extending the knowledge base of foresight: The contribution of text mining." Technological Forecasting and Social Change 116 (2017): 208-215.

Conferencing Tools

Conferencing tools are often used to involve participants from various geographic regions. They are extremely helpful for bringing together a diverse group of participants. However, we hypothesize that there is also a downside to using these tools. Participants may be less able to fully devote their attention to online meetings (as opposed to in-person workshops) due to the reduced interactivity of remote workshops and the fact that some individuals may be tempted to multitask or to join other meetings. Additionally, there may be varying levels of digital literacy within a group – due to a lack of technical skills and familiarity, some participants may not be able to fully and confidently participate while using a conferencing tool.

5. BEST PRACTICES

This chapter lays out best practices for planning and conducting foresight activities. The findings are primarily drawn from interviews but also include salient points from the literature review.

5.1 SUMMARY OF BEST PRACTICES

Scoping & Administration

Scoping is a critical step in the foresight process [69]. Whenever possible, it is recommended to identify a foresight organizer that has experience running foresight workshops and projects. In the initial scoping phase, the organizer begins to define objectives, foresight intention, time horizon, future handling approach, timeframe, required resources, etc. It is important to ensure that the objectives can be reached with the provided budget and resources.

In this stage of the project, the objectives of the activity should be well-defined (e.g., desired outcome, target audience, time horizon, stakeholders, key deliverables, communication and dissemination, etc.). It is also helpful to define objectives for each method or workshop - e.g., define a question for each STEEP factor.

In order to ensure maximum engagement, consider participant availability and key organizational or environmental milestones. For example, it is best to not plan events around times when participants are likely to be away on holiday. Furthermore, if the results of the foresight activity need to be provided to a key decision-maker, ensure that the findings can be delivered prior to major strategic meetings or events.

Finally, given that many foresight activities are regularly repeated, it is important to review results throughout the foresight project and at its conclusion. This provides an opportunity to learn how to improve future foresight activities.

Method selection

Since foresight activities rarely have straightforward goals or standardised outcomes, methods cannot be applied "*out-of-the-box*". Often, the methods to be used for an activity must be adapted to the goal and the scope of the activity, the context of the challenge, and even the participants involved. Foresight experts often see methods more as a frame of reference, which helps them to structure the activities.

Experts noted that creating a logical flow or frame for each foresight exercise, such as Design Thinking,[70] helps to focus on outcomes and to deliver a clear and concise plan. The frame may take the form of a modular building block approach, in which a variety of smaller blocks, each with a different focus (and method) are selected.

The methods mentioned in the example frame below demonstrate the range of possible methods - from foresight-specific (threatcasting) to more generic (role play). Frames can be grounded in existing frameworks or be simple process flows, like this illustrative one:

[69] A detailed description of the scoping process is provided by the EU Foresight Platform: http://www.foresight-platform.eu/community/forlearn/how-to-do-foresight/process/outcomes/

[70] Design Thinking is a user-centric problem-solving approach. For more information see: https://www.interaction-design.org/literature/topics/design-thinking

- understanding today (e.g., stakeholder or agent mapping/analysis, PESTLE[71]),
- detecting and defining changes (e.g., weak signals, trend analysis),
- articulating visions and futures into a coherent scenario (e.g., through scenario modelling: stories, visuals, roleplays) and
- analysing this future (e.g., threatcasting, scenario analysis, SWOT) to prepare recommendations.

Selecting a diverse participant group for foresight activities actively improves the group's capacity for creativity and ability to observe all facets of a topic.

In a well-designed foresight project, methods are carefully selected to form a diverse composition that best serves the objectives of the particular project and its participants. By using a frame, the objectives are well-defined, but the methods can be easily switched out as needed. The use of several methods allows for a range of topics to be addressed and increases the likelihood that each participant will provide pertinent input, thus eliciting the best outcomes for a foresight project.

Duration of foresight projects

The length of foresight activities is very versatile. They tend to span from four weeks up to one year and in some cases longer than a year. These longer-term activities are often used for continuous strategic planning but are less active and intense than shorter exercises. Long-term foresight is often assigned to a specific organizational role that is tasked with staying on top of new trends and deriving useful conclusions from that research. In these cases, work would also likely be divided into smaller, time-bound exercises.

For scenario modelling enthusiasts, there is a clear correlation between time invested and granularity (level of detail) of the scenarios. The main driver of this increase in granularity or quality of scenarios over time is introspective activity. Typically, a participant's capacity to understand the underlying systemic structure and possible evolutions or emergences increases over time; therefore, participants must be given sufficient time for introspection in order to ensure high-quality results.

A high level of granularity is often difficult to achieve in foresight activities, particularly for public sector actors, as scoping is particularly challenging at a national or regional level.[72] It is however possible to create valuable foresight results in a shorter time period. For example, in a crisis preparedness or response scenario, foresight can support a quick turnaround of actionable information; it will just not be as detailed as projects with more time and resources.

Participant Selection and Engagement

If possible, it is critical to ensure the involvement of the project's key stakeholders (e.g., the Head of Strategy) throughout the entire foresight process, including in smaller workshops. Delivering reports and outcomes at the end of the exercise is not as impactful for the readers as direct participation. In such a case, the findings of the exercise are less likely to be acted upon.

To ensure high-quality, well-rounded outcomes, a diverse group of individuals should be selected for participation. Diversity in this context will depend on the topic being analysed but may cover expertise, political affiliation, national origin or nationality, race, social class, gender, organizational role, age, etc. Ideally, all affected populations should be involved and represented in a foresight exercise.

Beyond the diversity of the group, it is also recommended to evaluate group dynamics when selecting participants. Characteristics that may be important to consider are shyness, ability to tolerate imperfection or lack of clarity, ability to express oneself in a group, power dynamics, etc.

[71] Note that there is the risk of investing too much time in this "understanding today" step of the process as participants may be more likely to believe that future outcomes will be analogous to the past. While information about past and current events or evolutions can be beneficial, they do not provide any indication that the future will follow similar patterns.

[72] Glod, F., Duprel, C., & Keenan, M. (2009). Foresight for science and technology priority setting in a small country: The case of Luxembourg. Technology Analysis & Strategic Management, 21(8), 933-951.

Consideration of this factor helps to ensure that the exercise remains productive and maximizes the engagement of all participants.

It may furthermore be beneficial to include generalists with a broad range of expertise as participants, as they can more easily provide a variety of perspectives. Likewise, it is often very important to include a participant with a strong legal background that can support the group in understanding the present, and likely future, legal constraints.

Communication & Engagement

Prior to the exercise, participants should be provided information such as: the goals of the exercise, the purpose of foresight (both in general and for the specific situation), the major components of the chosen method(s), and background on the specific topic, including any commonly used terminology that is crucial to the project (e.g., cybersecurity terms). If possible, the participants should be involved at the beginning of the activity in order to actively participate in shaping the project.

When communicating with a group of participants with varying areas of expertise, it has proven helpful to focus on outcomes over approach. Foresight is very rarely a person's full-time occupation, hence the need to provide the essential information without going into any unnecessary detail.

By giving participants a clear understanding of their role in the overall project, the exercise leaders are better able to manage any false assumptions and encourage a more unified participant group.

Time Horizon

Time horizon, the time frame a foresight activity aims to analyse, may be classified as **short-term or emerging** (0-5 years), **mid-term** (5-10 years), or **long-term** (10+ years). Definitions for time horizons do not always break down into these neat categories; we have adopted this categorization for the sake of clarity.

The choice of time horizon depends primarily on:

- the specific use case (e.g., climate change vs new technology)
- target objective (e.g., create a strategic plan, prepare response options)
- industry (fast moving (tech) vs long-term thinking (infrastructure))
- external factors (e.g., what is commonly reported on at your organization)
- and organizational or regional culture (are the participants accustomed to future-oriented thinking?).

The choice of time horizon should be tailored to each individual activity; nonetheless there are some notable characteristics for each time horizon to take into consideration.

While working with short-term time horizons, exercise participants tend to envision the future much like a simple linear extension of the present, and often have a hard time stepping outside of their own cognitive biases to envision futures different from the present (or commonly held expectations of the future.)

Long-term horizons allow people to free up their minds, but the plausible futures are very complex and speculative, as many factors need to be evaluated and weighed against one another. There is also often a lack of reliable data sources to support the participants' understanding of the distant future. Long-term time horizons are often used to move towards specific objectives – defining short-term responses that are likely to result in the intended consequence.

Mid-term perspectives seem to allow enough flexibility for participants to envision alternative futures that differ from the present, thus enabling the creation of creative strategies and near-term action plans.

5.2 SUMMARY OF CHALLENGES AND PITFALLS

Data Quality and Quantity

Accurate data may facilitate more reliable foresight results. Nonetheless**, data is always backward-looking**; any conclusions drawn from historical data should be evaluated for applicability to the future. In many cases there is a **surplus of data**, an analysis of which would overextend available resources and overwhelm the participants with data that is still, after all, from the past. Too much data may also restrict participants in their ability to participate creatively in the foresight workshops. Other times**, the data is either insufficient, or what is available is unstructured, or potentially unreliable**. In some technology-focused foresight activities, the participants' ability to consider ongoing innovations is limited due to lack of available information (often driven by concerns of intellectual property theft.) While this is to be expected, it can also negatively impact the outcomes of an activity. Moreover, one expert in the Working Group outlined four types of counterfactual information that may affect data reliability: gossip or rumours, fake news, rewriting of historical events, and frozen conflicts. These in turn often affect foresight exercises by warping the quality of the information and render fact-based consensus unlikely.

Participant Engagement

Regardless of how carefully participant groups are selected, there are often cases when chosen individuals do not fully participate in exercises or questionnaires. It is also difficult to get some participants to open up, think outside of the box, and embrace imperfection – all of which are critical for successful foresight activities. As mentioned above, however, these challenges may be minimized by clear presentation of the ultimate objectives and context of the exercise.

Cybersecurity-specific Challenges

Cybersecurity-specific foresight tends to focus heavily on specific technology and operational measures, limiting the ability to see strategically across the environment. Likewise, "game-changing innovations" are rarely easy to predict, but pivotal for assessing emerging and future cybersecurity threats. This is further complicated by the often confidential nature of the cybersecurity industry; experts may face a conflict of interest when supporting foresight activities. The current shortage of cybersecurity professionals may also be a challenge when planning and performing a foresight activity.

6. APPLICATION USE CASES

This section presents optional roadmaps for seven use cases identified by ENISA. The use cases represent a sample of how ENISA may apply foresight in the future. As mentioned in previous sections, the design of a foresight activity must reflect the reality of the contextual situation, resources, participants, etc. The processes proposed in this chapter are intended as a guide – in practice, the methods may need to be switched out or workshops added, for example.

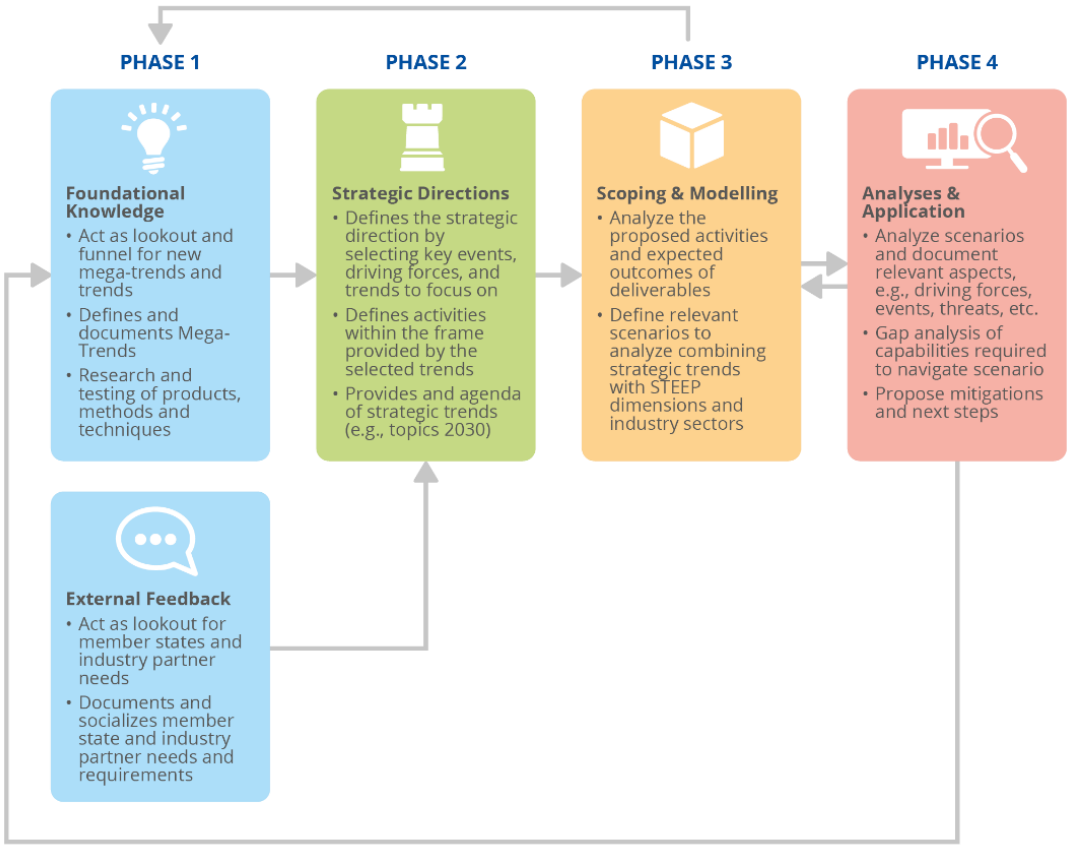
The use cases approaches described in the following chapter include:

1. **Identification of future and emerging challenges**
2. **Strategic decision-making development**
3. **Evolution of threat landscape**
4. **Needs and priorities for cybersecurity R&D**
5. **Evolution of operational cooperation**
6. **Identification of future policy priorities**
7. **Disruptive events**

6.1 OPERATIONAL CONTEXT

To better understand how foresight would be applied within ENISA, we held a workshop to identify major functions that would benefit from foresight. As a result, we mapped out a high-level structure of how foresight findings would flow between key functions within ENISA. This helped to identify dependencies between the use cases.

Figure 7: Understanding of ENISA's Operational Context



While ENISA's work is more of a continuous cycle, this depiction shows how the identification of emerging challenges and threats supports many activities such as strategy development, prioritizing research topics, and preparing recommendations for stakeholders. The use cases defined for each phase build upon one another, to maintain a continuous and sustainable information flow between organizational units and functions.

The use cases defined under each phase of the process are indicative - the activities and the deliverables are subject to ENISA's standard operating model and procedures, as well as the CSA (Cybersecurity Act), the main regulation that defines the mandate of ENISA.

6.2 OVERARCHING COMPONENTS AND CONSIDERATIONS

We have highlighted here some components common to all use cases.

Inception Phase & Scoping: Each activity must begin with the identification of scope, objectives, and stakeholders – it is critical to the success of the activity.

- Define the scope of the exercise (including contextual information such as the pertinent industry or EU scope).
- Identify and involve all stakeholders as early in the process as is possible. Expert Working Groups take time to put together (estimated min. 2 months), and many internal stakeholders may need to participate in multiple foresight activities.

Engaging with Participants: As these use cases often take place over a year, there is a chance that the participants will lose focus and interest in the activity.

- We recommend either maintaining frequent and regular contact with the participants or,
- Present an overview of the project's objectives and current findings before each part of the activity.

Tools: Some tools are needed for all use cases, such as:

- Video conferencing software
- Collaborative documentation tools (Confluence[73], Saga.so[74], Notion.so[75], etc.)

Resources: Where possible, the process recommended for each use case should build upon and make use of other foresight activities and reports.

[73] Please see https://www.atlassian.com/software/confluence
[74] Please see https://saga.so/
[75] Please see https://www.notion.so/

6.3 IDENTIFICATION OF FUTURE AND EMERGING CHALLENGES (1)

Each year ENISA works on reports identifying the future and emerging challenges relevant to their stakeholders. The reports themselves are used in many other aspects of ENISA's operations, therefore they must be both credible and actionable.

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

6.3.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Analyse current relevant social, technological, economic, environmental and political events.	Collect information on emerging trends and challenges from a variety of sources including, for example, market research firms, think tanks, academic publications, foresight research, etc. The STEEP method should be applied to ensure the comprehensiveness of the research itself. Research and findings are to be shared amongst participants and experts for feedback. If ENISA is conducting its own data analysis, Trend Intra- & Extrapolation may be used to project future outcomes based on historical data. This will be the most time-intensive step.	STEEP PESTLE Literature Review Trend Interpolation & Extrapolation Desk Research
2	Identify and document possible change events and future states.	Gather internal and external (expert) stakeholders to conduct a brainstorming workshop. In the workshop, all participants will write down change events and systemic emergences that they have noticed or have studied for each category (STEEP). The group discusses the results, adds findings from the desk research, and together creates a shortlist of trends to investigate further. The trends are divided amongst participants to collect further information.	Brainstorming
3	Identify and document driving forces of change for the predicted events in each PESTLE category.	To identify a driving force of change, analyse all the events which have been brainstormed in the previous phase and locate causal dependencies amongst them. Relationships or dependencies between events should not only have a cause-and-effect nature. The analysis should include the technologies, social attitudes, political positions and actors or interest groups acting as facilitators or perpetrators of the events. The workshop(s) should rely on an expert group composed of a diverse range of participants (e.g., cybersecurity professionals, economists, psychologists, sociologists, etc.).	Causal Layered Analysis (CLA)
4	Identify cybersecurity topics related to drivers and change events in each PESTLE category.	Based on the information generated during previous steps, experts participating in the workshop must identify cybersecurity related topics. This is performed by looking at the current environment, the predicted evolutions or change events, driving forces for the changes, and possible end states through the lens of cybersecurity.	Brainstorming
5	Categorize and prioritize topics and drivers based on speed of evolution and impact on cybersecurity.	After gathering relevant cybersecurity topics in step 4, an internal working group of ENISA experts should review, complement and categorize the topics. The categorization narrows the focus of the ENISA team to only relevant topics. From there, the team may derive future activities such as further exploration, training exercises, policy recommendations, etc.	Participatory Design

6.4 STRATEGIC DECISION-MAKING DEVELOPMENT (2)

ENISA relies on solid, fact-based strategic decision-making to decide how to allocate resources, plan future activities, and identify areas of development. Foresight activities enable the leadership to design a strategy that can manage future challenges.

Category	Description
Objective	Guide the strategic planning process to validate the assumptions and the level of ambition; review principles, priorities and requirements for the Agency to realise its vision and fulfil its mission.
Deliverable	Revision of ENISA strategy document(s)
Time Horizon	3-5 years
Collaborating Stakeholders	ENISA Internal; ENISA Management Board and Advisory Group
Target Audience	ENISA Stakeholders & Management Team
Impact on Target Audience	Modify strategic decision-making actions
Level of Granularity	High-level strategic guidance,[76] directions, and priorities
Time to Conduct Exercise	1 year
Dependencies	All other use cases

[76] For more information on using foresight to provide policy guidance see the work of Lieve Van Woensel: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690529/EPRS_BRI(2021)690529_EN.pdf

6.4.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Review and update relevant research and current environmental factors.	Using the Future & Emerging Challenges and Threat Landscape reports as a basis, initiate a focused desk research phase structured by the STEEP analysis. During this phase, the emphasis would be identifying any developments that have emerged since the workshops conducted as part of other use cases. Research and findings are to be shared amongst participants and experts for feedback.	STEEP PESTLE Literature Review
2	Review the documentation and explore additional scenarios which may be desired, disruptive and/or likely to happen.	Scenario Planning: Based on the information collected in Step 1, identify possible futures that ENISA would be a part of. The focus should be on very disruptive or probable futures; this ensures that the resulting strategy is flexible enough to accommodate many possible outcomes. In this step, the participants would create a rather long list of potential scenarios that would be shortlisted in the next step. Expert Workshop: Scenarios produced in the previous step should be reviewed with the expert group to identify clusters which warrant further exploration, based on their potential for disruption or likeliness of emergence. Within an internal ENISA group, a desired future should be selected that can guide strategic initiatives.	Scenario Method Brainstorming
3	Model relevant scenarios of the future.	It is recommended that relevant scenarios or clusters be modelled at this point, exploring different aspects such as PESTLE or STEEP context and situation, day-to-day experience for actors living in the future scenario, group or individual motivations, desires and needs, consumption habits, etc. The scenarios can be further explored with the expert group by engaging in iterative design practices through a series of workshops, improving the level of granularity of the descriptions and the understanding the experts develop on the future state.	Scenario Method
4	Define a normative vision of ENISA for these futures.	Create a normative vision: Hold a workshop to identify ENISA's ideal role in shaping the desired future(s). Using the modelled scenarios, identify the role that ENISA wants to play in each of the chosen futures. How does that look and how does it reflect to ENISA's core values and mandate? What are ENISA's responsibilities in this alternate future?	Scenario Method Visioning Backcasting
5	Backcast initiatives required to reach the normative vision.	In a workshop with internal stakeholders (and external consultants as needed), brainstorm possible initiatives to reach the normative vision. For example, how would ENISA fulfil its mandate in such a future? What steps would ENISA need to take now to help shape the situation towards the desired future? It is important to remember that the identified tasks and initiatives need to allow for the possibility that another, more disruptive, future may arrive.	Backcasting
6	Define an evolution roadmap and complete the strategy with guidelines and principles.	Prioritize and organize the initiatives needed to achieve and accommodate alternate futures. Based on the roadmap identify common themes and guiding principles to support the strategy. Incorporate both overarching themes and specific initiatives into the strategic document.	Roadmapping

6.5 EVOLUTION OF THREAT LANDSCAPE (3)

Each year, ENISA publishes their analyses on the European threat landscape.[77] This is an important aspect of much of ENISA's work as the most prevalent threats may also drive the Agency's priorities and strategy.

Category	Description
Objective	Produce an overview and analysis on emerging threats and drivers, to inform the general public and cybersecurity professionals. (report)
Time Horizon	1-3 years
Collaborating Stakeholders	ENISA Working Group & other EU agencies
Target Audience	General public, policymakers, cybersecurity professionals
Impact on Target Audience	Stay up to date on emerging threat landscape; begin preparations and measures to address emerging threats
Level of Granularity	Specific cybersecurity threats and trends
Time to Conduct Exercise	6-9 months
Dependencies	

[77] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

6.5.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Analyse current environment for existing threats and threat actors.	Environmental Scanning: Initiate a short desk research phase focused on security event and incident reports, as well as cybersecurity threat analyses from the previous year. Research and findings are to be shared amongst participants and experts for feedback. Other tools such as data mining may be used to identify threat methods or attack vectors that are on the rise. Expert Panel: Alongside the Context Gathering step, gather a diverse group of experts to provide input on potential threats. The Expert Panel (typically 12-20 people) may be divided into groups based on areas of expertise or focused on a particular threat category (e.g., ransomware attacks). This could be a longer phase (>3 months) or shorter, depending on the timeline of the project and resources available.	Desk Research PESTLE Expert Panel
2	Identify drivers for actors and threats.	Expert Workshop: For the identification of the underlying causes of threats and motivations of threat actors, a diverse group of participants should be assembled, including profiles such as psychologists, sociologists, economists, technology experts, cybersecurity enthusiasts, etc. The participants should use tools such as personas and empathy maps to understand the motivations of the threat actors, as well as their ultimate goals.	Stakeholder Mapping Personas Empathy Map Causal Layered Analysis
3	Trend Analysis: Identify and document possible change events and future states.	Combining desk research and workshop format (Trend Mapping), the participants would identify change events that are impacting the major threats and threat actors. These should be distinct from threat events (i.e., the rise of insider threat would not be a change event, rather that the COVID-19 pandemic weakened social ties within organizations).	Trend Mapping Brainstorming Mind maps
4	Identify and document future threats.	Threat Identification and Comparison: This activity may then be extended by the Threat Agent Risk Assessment (TARA) method.[78] The participants will compare their research and structure it into lists of threat actors, attacker objectives, and attack methods. This method offers a way of getting an overview of threat actors, their objectives, and attack methods and narrowing it down to the most high-risk or novel threats. The TARA method is typically used to assess the major risks to an organization, country, etc. but it may also be used to identify how new methods or change events may lead to novel threats.	TARA Thought Experimenting Desk Research
5	Propose and document recommendations.	In a workshop with cybersecurity professionals, categorize and prioritize threats. Obtain feedback in iterative rounds.	Participatory Design

[78] Threatcasting was not recommended purely because it is designed for a time horizon of 10 years. For more information on TARA, see Rosenquist, M., Prioritizing Information Security Risks with Threat Agent Risk Assessment, Intel Information Technology, USA, 2009.

6.6 NEEDS AND PRIORITIES FOR CYBERSECURITY R&D (4)

ENISA provides a valuable service by identifying areas within the field of cybersecurity in need of development. This use case builds on the previous three to reach a greater degree of granularity. Research and development may also inform future strategic decision-making or may serve as inputs for environmental scanning.

Category	Description
Objective	Analyse gap between existing research focus and required future focus based on landscape evolution
Deliverable	Gap analysis and recommendations
Time Horizon	1-5 years
Collaborating Stakeholders	Research community
Target Audience	Research community, Competence Centre, European Commission (EC)
Impact on Target Audience	Enables the ability to identify future research and innovation needs; contributes to the Competence Centre Strategic Agenda and Work Program; Contributes to the EU Strategic Agenda on Research and Innovation
Level of Granularity	Detailed – needs to produce concrete direction
Time to Conduct Exercise	6 months
Dependencies	Identification of Future and Emerging Challenges; Evolution of threat landscape

6.6.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Research & Environmental Scanning	Using the Future & Emerging Challenges Report as a basis, initiate a short desk research phase structured by the STEEP analysis. During this phase the emphasis would be identifying any trends, threat actors, or technologies that were not covered in the Challenges Report. Research and findings are to be shared amongst participants and experts for feedback. If ENISA is conducting its own data analysis, Trend Interpolation & Extrapolation may be used to project future outcomes based on historical data.	STEEP Trend Interpolation & Extrapolation Bibliometrics Text Mining Literature Review
2	Identify and document possible change events and systemic emergences.	Gather internal and external (expert) stakeholders. In a workshop, all participants will write down change events and systemic emergences that they have noticed or have studied for each category (STEEP). Afterwards they should: discuss results of the workshop, incorporate desk research findings, shortlist trends to investigate, and delegate trend research to participants.	Scenario Method Expert Panel Brainstorming Desk Research
3	Identify driving forces for possible change events and emergences.	To identify a driving force of change, analyse the events brainstormed in the previous phase with a diverse expert group and locate causal dependencies amongst them.	Personas Causal Layered Analysis
4	Transform driving forces into bipolar factors and combine to identify alternate futures.	Once the driving forces have been identified, the project team should define bipolar factors for each driver (desk research or internal workshop.) A bipolar factor is a construct based on a driving force, stating an “either/or” outcome in the future. For example, if the driving force is “general social desire to optimize the ownership of assets”, then the bipolar factor should focus on attitudes towards possession, with full or partial ownership or full usership (full transformation of social paradigm) as possible outcomes. By defining a series of bipolar factors and using a combinatorial approach, a scenario modelling team can create a set of scenarios, based on the “either/or” outcomes defined for each bipolar factor. For example, if an exercise has defined two bipolar factors, a total of 4 scenarios would be created.	Scenario Method Bipolar Factors
5	Identify, explore and model highly relevant scenarios.	The scenarios should then be reviewed with the expert group to identify clusters that warrant further exploration based on their potential for disruption or likeliness of emergence. Model the relevant scenarios or clusters, exploring different aspects the environmental context and situation, day-to-day experience for actors living in the future scenario, group or individual motivations, desires and needs, consumption habits, etc. The scenarios can be further explored through iterative design workshops that increase the level of granularity of the descriptions and experts’ understandings of the future.	Scenario Method
6	Identify relevant cybersecurity topics and drivers in most relevant scenarios.	Part of the scenario modelling exercise should also focus on the cybersecurity aspects governing the future state. Topics such as technologies, threats, threat actors, etc. should be regularly explored. Existing threat landscapes (see Use Case 3) can be used as input.	Threat Modelling

7	Prioritize topics and drivers based on cross-scenario frequency.	ENISA stakeholders should then review the modelled scenarios to canvas for relevant topics from a cybersecurity point of view. The analysis can be performed by identifying topics which have a high frequency and impact across several scenarios.	Scenario (2x2) Matrix
8	Review current research and identify gaps.	Review ENISA strategy and research topics currently in focus. Analyse gap between relevant topics identified in the future scenario which might warrant further research focus and current topics being researched.	
9	Propose new research topics.	Construct recommendations to expand research and innovation agenda. The findings may be reported to research partners across disciplines.	

6.7 EVOLUTION OF OPERATIONAL COOPERATION (5)

Operational cooperation is one the ENISA strategic objectives: by coordinating both the secretariat of the EU CyCLONe and the EU CSIRTs Network, ENISA aims to synchronise technical and operational levels as well as all EU actors in order to collaborate and respond to large scale incidents and crises. The evolution of operational cooperation must consider a variety of factors that are constantly shifting. Integrating foresight into this process will help to understand the possible futures of operational cooperation.

Category	Description
Objective	Produce analysis and recommendations on cooperation mechanisms and relationships
Deliverable	Report on the evolution of operational cooperation bi-annually.
Time Horizon	1-3 years
Collaborating Stakeholders	Blueprint Actors
Target Audience	Blueprint Actors
Impact on Target Audience	Understand relevant driving factors for a specific threat or crisis, as well as the possible cooperation mechanisms to improve cybersecurity response
Level of Granularity	High-level
Time to Conduct Exercise	1 year
Dependencies	Evolution of Threat Landscape

6.7.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Analyse and document threat landscape, attack trends, etc.	Using the Future & Emerging Challenges and Threat Landscape reports as a basis, initiate a desk research phase structured by the STEEP analysis and focused on the factors relevant for operational cooperation. During this phase the emphasis would be on identifying any trends, threat actors, or technologies that have emerged since the workshops conducted as part of use cases 1 and 3. Research and findings are to be shared amongst participants and experts for feedback.	PESTLE STEEP Trend Maps
2	Analyse existing cooperation structures and resilience levels.	Analyse and document existing cooperation mechanisms and structures, as well as notable events that demonstrated a successful or failed cooperative activity (desk research). In a stakeholder workshop, compare findings and categorize them into structural or thematic components. Interviews with individuals with operational responsibility may also provide valuable insight (if time and resources allow).	Stakeholder Maps Mind Maps Personas
3	Identify and document gaps in existing cooperation relationships and mechanisms.	Based on the findings from the previous steps, identify gaps in the operational cooperation infrastructure. These may be prioritised by using a risk assessment method or in a separate workshop with a diverse group of individuals associated with the Blueprint Actors.	Risk Assessment World Cafe
4	Propose and document cooperation relationships and mechanisms required to increase resilience.	Taking the findings from the previous two steps, conduct a workshop (or a series of workshops) with experts to identify mechanisms to strengthen operational cooperation. Findings may then be iteratively revised within an internal/Blueprint Actor feedback loop.	Brainstorming Thought Experimenting World Cafe

6.8 IDENTIFICATION OF FUTURE POLICY PRIORITIES (6)

As a trusted advisor of policymakers, ENISA provides overviews of emerging challenges that may warrant a policy response.

Category	Description
Objective	Produce an overview and analysis on emerging and future topics and drivers, to inform policy making entities and actors.
Deliverable	Opinion / High-level overview of emerging and future topics
Time Horizon	3-5 years
Collaborating Stakeholders	Policy Observatory Expert Group
Target Audience	Policymakers
Impact on Target Audience	Be informed of emerging and future trends that warrant assessment in terms of relevant policy interventions
Level of Granularity	General trends and directions, generic topics. Emerging and future topics to be analysed from a policy perspective, with additional information from the Research and Innovation Team where needed.
Time to Conduct Exercise	1 year
Dependencies	Identification of Future and Emerging Challenges; Evolution of threat landscape

6.8.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Review and update relevant research and current environmental factors.	Using the Future & Emerging Challenges and Threat Landscape reports as a basis, initiate a desk research phase structured by the STEEP analysis. During this phase the emphasis would be identifying any trends, threat actors, or technologies that have emerged since the workshops conducted as parts of use cases 1 and 3. Research and findings are to be shared amongst participants and experts for feedback. Alongside the Context Gathering step, gather a diverse group of experts to provide input on both the existing policy landscape and the identified future challenges and threats. The Expert Panel may be divided into groups - based on areas of expertise or focused on a particular topic or factor within STEEP.	STEEP PESTLE Desk Research
2	Identify and document possible change events and future states.	Gather internal and external (expert) stakeholders to conduct a brainstorming workshop. In the workshop, participants will write down possible change events and systemic emergences that they have noticed or have studied for each STEEP category. Afterwards they should: discuss results of the workshop, incorporate desk research findings, shortlist trends to investigate, and divide up trend research tasks.	Expert Panel
3	Identify and document driver(s) of change for predicted events.	To identify a driving force of change, analyse all events collected in the previous phase and locate causal dependencies amongst them. The workshop(s) should rely on a diverse expert group.	Brainstorming World Cafe
4	Identify topics related to drivers and change events.	After identifying driving factors, select topics that are particularly salient to policymakers. These topics may be derived from any step of the foresight process.	Desk Research Causal Layered Analysis
5	Analyse topics and identify gaps in regulation or policy. Propose areas of focus and recommendations for policy development.	Core stakeholders will collect the findings from the previous phases and identify possible gaps in the policy landscape or provide guidance on key factors to consider in the policymaking process. These conclusions need to be validated in feedback loops with experts and internal stakeholders.	Participatory Design

6.9 DISRUPTIVE EVENTS (7)

As demonstrated by the COVID-19 pandemic, transformational events or situations can occur suddenly and without warning. In those cases, it is prudent to have a structured process with which to generate possible outcomes. This supports decision-makers and brings additional clarity to entities that may need to support in such a crisis situation. Examples of these events could include, for example, mass ransomware incidents (like NotPetya) or wide-reaching APTs (advanced persistent threats).

Category	Description
Objective	Envision possible future states following a large disruptive event.
Deliverable	Scenarios describing possible future states (Lines to Take or LTTs)
Time Horizon	2 – 4 weeks
Collaborating Stakeholders	ENISA Internal; Key Member States Stakeholders; Cybersecurity Experts
Target Audience	ENISA Stakeholders & Management Team
Impact on Target Audience	Provide an overview of the impact of disruptive events and outlook of possible future states in order to inform organizational response and capabilities allocation.
Level of Granularity	Key driving factors and forces, emerging events, possible alternate future states
Time to Conduct Exercise	A few days
Dependencies	None

6.9.1 Foresight Approach

#	Process Step	Detailed Description	Recommended Methods & Tools
1	Define scope of analysis	Review disruptive chain of events and identify main (visible) triggering event.	
2	Sensemaking of event	Analyse the main disruptive event and identify early signals, main actors and STEEP impacts on current environment (only what can be seen right now)	Stakeholder Map STEEP
3	Identify emergences and event dependencies	Identify emerging events and event chains, stakeholder and actor reactions and strategies to cope with disruptive event. Identify at least three possible reactions per stakeholder or main actor.	LEGO Serious Play[79] – Application technique 6: Playing Emergence
4	Scenario identification	Identify and name scenarios through combination of identified chains of events and main actor reactions/strategies. Select chains of events that are plausible, possible and probable and combine stakeholder or actor reactions to generate a long list of scenarios.	Scenario Method
5	Scenario prioritization	Discard implausible scenarios and evaluate the probability and possibility of remaining scenarios using a two-by-two matrix.	2-by-2 matrix
6	Scenario deep dive	Review highly possible and probable scenarios and explore internal dynamics of each. Define scenario stories - detail context, stakeholder or actor actions, STEEP aspects and other relevant aspects required by ENISA management. Model the relevant scenarios or clusters, exploring different aspects the environmental context and situation, day-to-day experience for actors living in the future scenario, group or individual motivations, desires and needs, consumption habits, etc. The scenarios can be further explored through iterative design workshops that increase the level of granularity of the descriptions and experts' understandings of the future.	Scenario stories STEEP

[79] For an introduction and overview of LEGO Serious Play, see Frick, Elisabetta & Tardini, Stefano & Cantoni, Lorenzo. (2013). White Paper on LEGO ® SERIOUS PLAY A state of the art of its applications in Europe.

7. CONCLUSIONS & NEXT STEPS

7.1 CONCLUSIONS

Foresight can be an asset to the cybersecurity community

Cybersecurity often looks towards future short-term threats, yet there is a need for cybersecurity professionals and policymakers to maintain pace with attackers. Foresight is a good tool for supporting longer term strategic thinking on how to improve the state of cybersecurity and overall resilience. ENISA is taking an important strategic step to better integrate foresight into cybersecurity practices.

Foresight is flexible and must be adapted for each activity

At the beginning of each foresight project, the methods and tools used should be thoughtfully chosen and/or augmented to best suit each unique context and group. Even ongoing activities may be updated with lessons learned. For example, if after one workshop the objectives were not achieved the format of the following workshop should be adapted to suit the context and participants. The recommendations in this report are not prescriptive and should be adapted as needed.

Where possible, engage one or more foresight experts for critical activities

Experts have the experience to select methods that best fit the group, but they also have more knowledge of the more indefinite aspects of foresight – attitudes, framing, ethics, etc.

Foresight is an opportunity to improve understanding and communication

When stakeholders are involved in a foresight process, they obtain a wealth of information and also face the challenge of how to transport ideas and possibilities in an easily comprehensible way. This is an excellent exercise to develop staff members and leadership alike.

7.2 NEXT STEPS FOR ENISA

Design and Resource Allocation

The most pivotal step will be to design the foresight activities themselves – including participants, timelines, etc. The more aligned the activities are to the organization in the design phase, the less likely that significant changes will be needed after testing the foresight activity approaches. It is also notable that resource allocation is critical for determining basic elements of planned activities - the number of participants, timeline, and if a foresight professional can be brought in to lead the activity.

Test and Adapt

To fully utilize the potential of foresight at ENISA, it needs to be tested in a variety of teams, settings, and contexts. Testing enables ENISA to align the foresight approach to our specific needs, thus easing the process of integrating foresight into operational work. Foresight needs to be integrated integrated into processes in order to figure out the best set up and timeline for the organization. In doing so, ENISA may create a culture of foresight which in turn increases the quality of foresight outputs.

Collaborate with Key Stakeholders

ENISA's foresight activities may be enhanced by drawing upon the expertise of and collaborating with other European (or MS) agencies and institutions that conduct foresight.

Support Build Up of Foresight Capability

Foresight can be useful in many contexts and would be an asset for strategic cybersecurity planning for EU Member States. ENISA's lessons learnt and new expertise could be useful to get national foresight programs off the ground.

A ANNEX: GLOSSARY

Design Thinking	A user-centric problem-solving approach[80]
Foresight	Foresight is a systematic, participatory, future intelligence-gathering and medium-to-long-term vision-building process aimed at enabling present-day decisions and mobilizing joint actions[81]
Framework	A set of principles and processes containing method with tools, aimed at solving complex challenges
Granularity	The level of detail or quality of something[82]
Method	A multi-step procedure aimed at solving a specific challenge
Organizational Capability	The capacity of performing activities or executing processes to achieve organizational goals[83]
Time Horizon	A fixed point in time in the future which a foresight activity aims to analyse
Tool	A predefined template to structure information

[80] See https://hpi-academy.de/en/design-thinking/what-is-design-thinking.html
[81] See Miles, I., Keenan, M., *Practical Guide to Regional Foresight in the UK*, Publications of the European Communities, Luxembourg, (2002).
[82] See https://dictionary.cambridge.org/dictionary/english/granularity
[83] See https://smallbusiness.chron.com/importance-organizational-capability-13295.html

B ANNEX: INTERVIEW GUIDELINE

Introduction

1. Please describe your current role and summarize your experience with foresighting [84]methods.
2. Please summarize your experience with cybersecurity. We would be interested to know if you have applied foresight methods for cybersecurity topics.

Foresighting methods and Evaluation

3. In what context do you apply foresighting within your profession?
4. For which time horizon do you typically use foresighting for?
5. Which foresight methods do you use?
6. How do the methods you mentioned relate to the foresighting needs of your profession?
7. What are the criteria you apply to select a foresighting method in the context of your profession?

Foresighting Activities Example

8. Please describe a typical foresighting activity for you – who is involved, how long is the process, diversity of groups
    a. How long does it take to deliver results based on the foresighting activities that you mentioned?
    b. Do you use any specific technology-based tools or databases to support your foresighting activities?
    c. How much time do you need to invest in order to achieve the expected granularity / quality? (Are some methods more efficient than others?)

Lessons Learned

9. What are some lessons learned you have gathered about conducting foresighting activities?
    a. What challenges have you encountered with the methods you mentioned or have used in the past?
    b. What challenges have you encountered with running foresighting exercises (e.g., participant interaction)?
    c. What are specific pitfalls you find when foresighting for short-, mid- and long-term timeframes?
    d. Have any tools (especially for remotely run foresighting activities) proved helpful?
    e. Is there any terminology you use that has been beneficial for introducing methods to non-expert groups?
    f. If you use foresighting for cybersecurity, did you find any specific challenges or lessons learned for this activity?

[84] Initially, the team used the term “foresighting”, but this is not as commonly used as “foresight.” While other aspects of the report have been adapted, “foresighting” is maintained here for accuracy.

TP-06-21-178-EN-N-

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-546-3
doi: 10.2824/187824