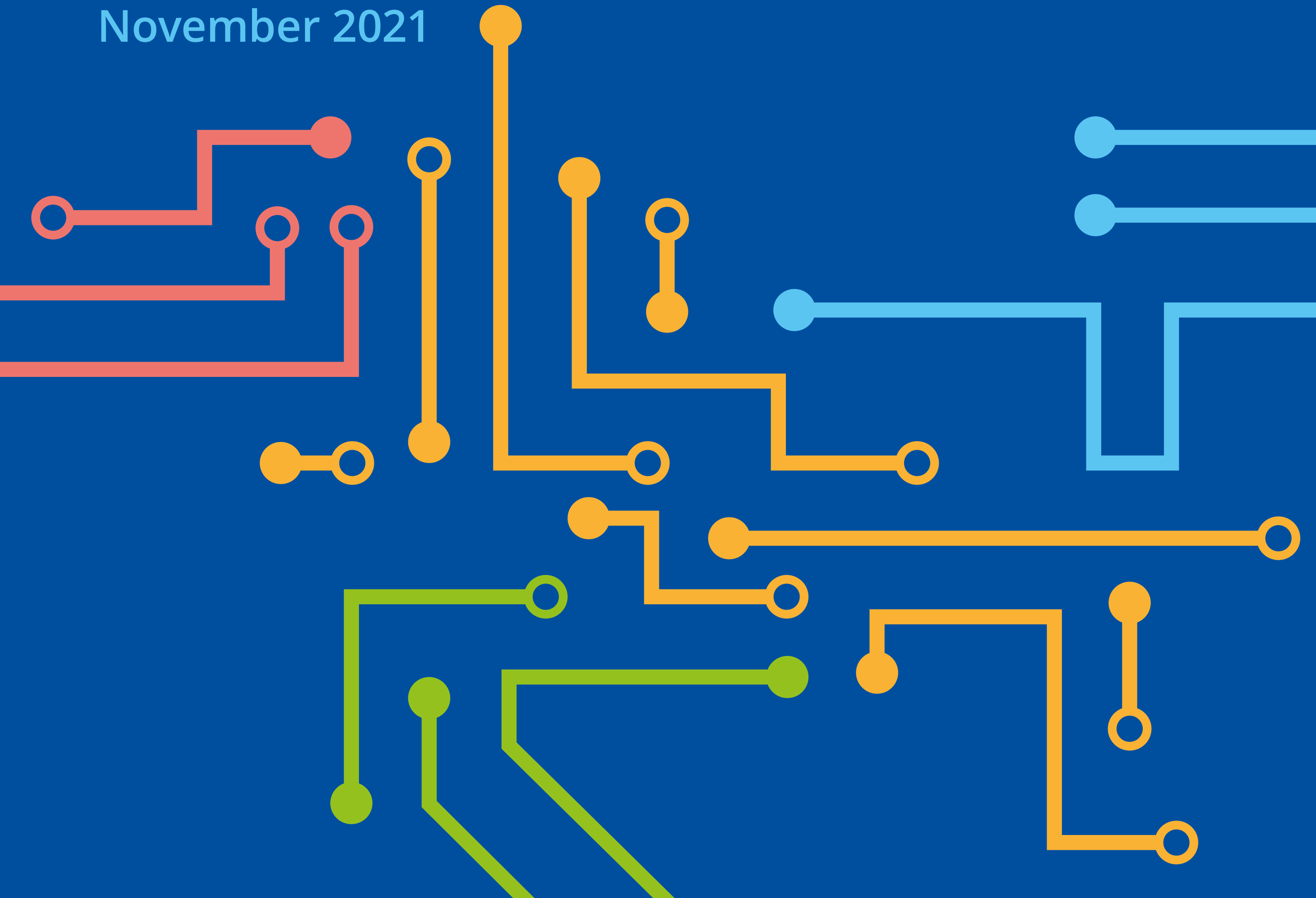
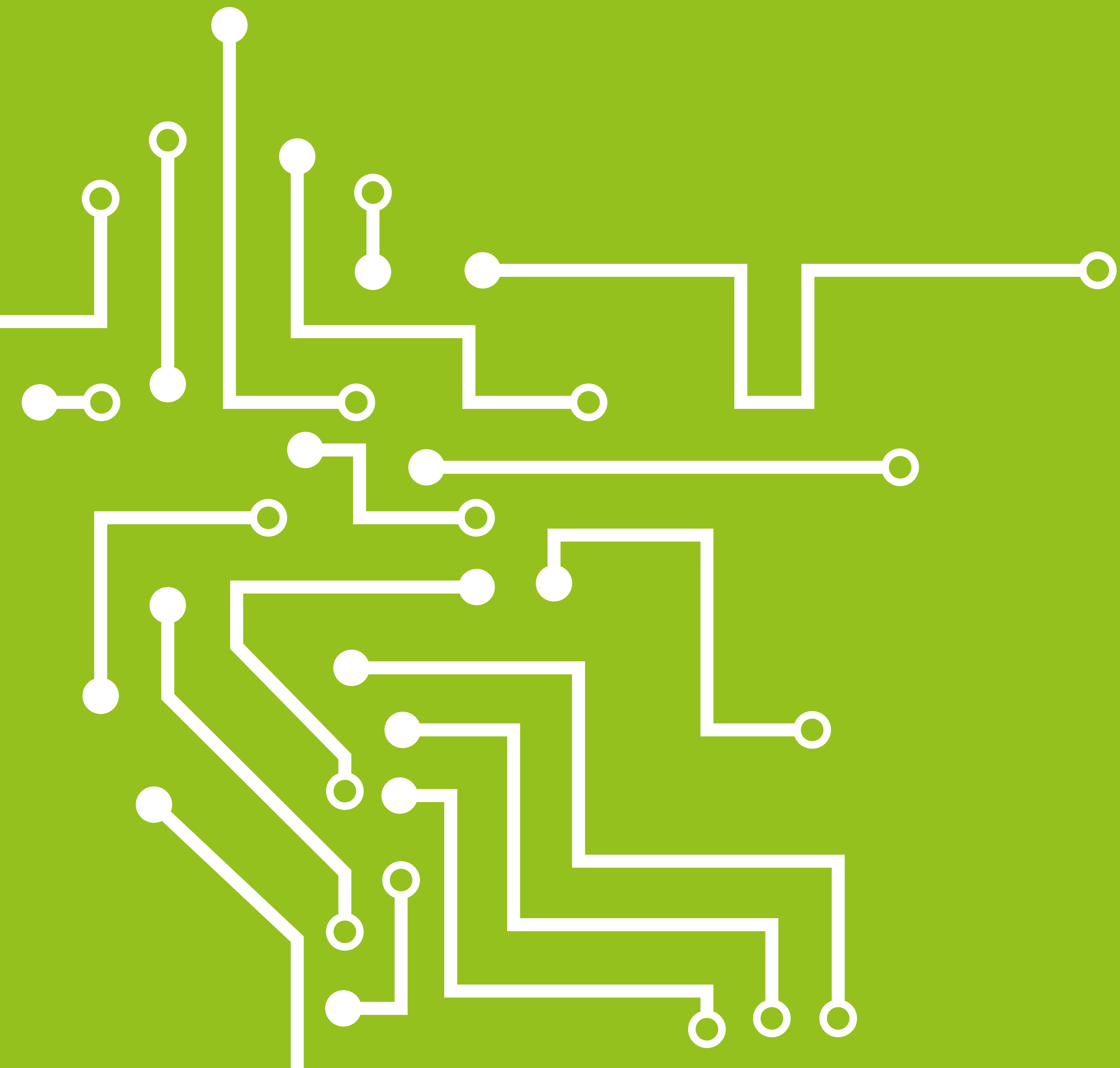
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INTERNATIONAL STRATEGY

OF THE EU AGENCY FOR CYBERSECURITY

November 2021





INTRODUCTION

1.1 Article 12 of the Cybersecurity Act (CSA) states that 'ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on issues related to cybersecurity' in various ways, including facilitating the exchange of best practices and providing expertise, at the request of the Commission.

1.2 Article 42 of the CSA requires the Management Board of ENISA to adopt 'a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent' ([1]). The CSA also refers to specific international organisations (e.g. Organisation for Economic Co-operation and Development (OECD), Organization for Security and Co-operation in Europe (OSCE) and North Atlantic Treaty Organisation (NATO)) that ENISA is called to develop relations with (see recital 43).

1.3 Since the entry into force of the CSA, ENISA's exposure to partners outside the EU has increased both quantitatively and qualitatively ([2]). ENISA is also often approached by third countries directly with high expectations of mutual collaboration, and is confronted each time on how best to react. Such welcomed developments call for a more strategic approach to the international dimension of ENISA's work in order to guide the engagement of the Agency with third country partners, as well to direct Agency's response to third country partners seeking cooperation with ENISA.

1.4 This international strategy covers the cooperation with international organisations and with non-EU countries. However, for those non-EU countries or regions with which the EU has special agreements this international strategy should be read in the light of such agreements, looking at where a closer cooperation in the area of cybersecurity is foreseen.

[1] Chapter II of Title II of the CSA covers all tasks of ENISA and thus outlines areas in which ENISA is competent.

[2] The expectations of various actors inside the EU institutions and of Member States for ENISA to engage more actively internationally have increased, as was stressed in the bilateral interviews undertaken by ENISA in spring 2021. This was also confirmed in the internal survey carried out by ENISA in early 2021.

ENISA'S OVERALL INTERNATIONAL APPROACH

The directions and provisions in this strategy will not in any way limit or hamper the provisions laid out by Article 12 of the CSA.

The mandate of the Agency is to achieve 'a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity'. Under this mandate, ENISA's strategic aim is to build a trusted and cybersecure Europe. ENISA's international strategy must therefore be at the service of the Union, advance the achievement of the Agency's mandate within the Union and contribute to its strategy ([3]).

[3] ENISA (2020), A Trusted and Cyber Secure Europe – ENISA strategy (https://www.enisa.europa.eu/publications/corporate-documents/enisa-strategy-a-trusted-and-cyber-secure-europe).

This underlying premise directs the Agency to be selective in engaging with international partners and to limit its overall approach in international cooperation to only those areas and activities that will have high and measurable added value in achieving the Agency's strategic objectives.

International cooperation should be resourced prudently and proportionally. This strategy outlines three approaches that the Agency can use in terms of level of commitment of resources: the limited, assisting and outreach approaches.

2.1 LIMITED APPROACH

ENISA's default international approach is 'limited'. Under this approach, ENISA will, in line with its objectives enshrined in Article 4 of the CSA, exchange information with relevant international partners on an ad hoc basis ([4]), to strengthen and develop its expertise and anticipate changes prompted by global developments in cybersecurity. It will seek to promote the Union's values and to advance its strategic objectives and cybersecurity policies when engaging with international partners in meetings, conferences and seminars. ENISA will not commit dedicated resources to pursue this approach beyond mission or conference costs.

2.2 ASSISTING APPROACH

In line with its mandate to 'actively support Member States, Union institutions, bodies, offices and agencies in improving cybersecurity' (Article 3(1) of the CSA), ENISA may respond to requests for assistance – when the request is deemed to add significant value to a specific strategic objective and is in line with the Union's policies – namely from third countries and international organisations with which the Union has agreements or frameworks that promote specific or general cooperation in cybersecurity. Under this approach, ENISA may exchange and share expertise, contribute to organising training sessions and exercises, support the Commission/EU in building and maintaining cybersecurity dialogues and support individual cybersecurity activities with international partners organised by the requester. To respond to such requests, ENISA might use resources dedicated to specific strategic objectives as set out in its single programming document (SPD).

2.3 OUTREACH APPROACH

ENISA may follow an 'outreach' approach for specific aims and provisions of the strategic objectives outlined in this strategy, to proactively engage with specific international partners to be able to advance the Agency's strategic objectives and fulfil the objectives of the CSA. Under this approach, ENISA may plan dedicated resources in its SPD in pursuit of this approach.

[4] For principles that govern selecting and engaging with international partners, please see Section 3 of this annex: 'Principles governing ENISA's international approach'.

PRINCIPLES GOVERNING ENISA'S INTERNATIONAL APPROACH

1. ENISA will focus its international cooperation on partners with which the Union has strategic economic relationships and which share the Union's values.

2. When cooperation in cybersecurity between the Union and an international partner is explicitly stated in an agreement, ENISA may follow an outreach approach, respecting the limits of the agreement provisions.

3. Beyond specific provisions outlined under Section 4 of this annex, 'Specific aims and provisions under individual strategic objectives', ENISA can, when relevant, pursue an outreach approach across all of its strategic objectives with European Economic Area countries.

4. ENISA will refrain from engaging with international actors if contacts or cooperation with such actors would be deemed incompatible with the Union's interests or policy goals.

5. The Agency's international cooperation activities should align with and add value to the partnerships of Member States.

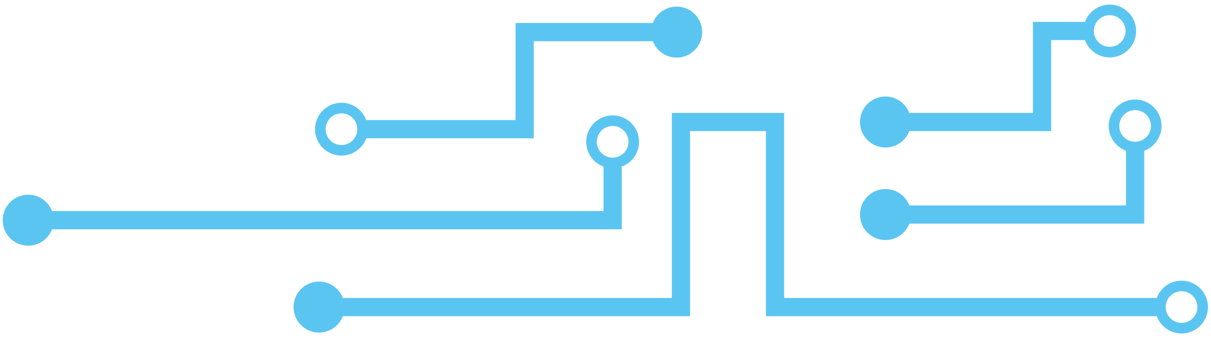
6. When responding to requests under the assisting approach not explicitly covered in this strategy, and where otherwise appropriate, ENISA will consult and coordinate with the European External Action Service and the Commission, to ensure that the Agency's international engagement is in line with the Union's policy goals. ENISA will notify the Executive Board of requests under an assisting approach and those under an outreach approach. ENISA will furthermore ensure that its outreach activities are in line with the Union's policies by regularly consulting with the Directorate-General for Communications Networks, Content and Technology.

7. In its SPD, ENISA will proportionally evaluate the resources needed for involvement in any international activities with an assisting or outreach approach.

8. ENISA will seek endorsement of the Executive Board prior to developing cooperation frameworks or agreements with international organisations and third countries. When such agreements place financial or legal obligations on the Agency, they must be approved by the Management Board.

9. In its annual activity report, ENISA will outline all international activities it has pursued under different approaches. In particular, it will evaluate and provide assessment of the added value of international activities under an assisting or outreach approach in pursuit of its strategic objectives.

10. The Agency should be able to react in an agile manner while adhering to these principles.



SPECIFIC AIMS AND PROVISIONS UNDER INDIVIDUAL STRATEGIC OBJECTIVES

4.1 STRATEGIC OBJECTIVE ‘EMPOWERED AND ENGAGED COMMUNITIES ACROSS THE CYBERSECURITY ECOSYSTEM’

ENISA exchanges best practices and expertise and promotes international activities to enhance the cybersecurity awareness and education of the various communities of the Union. Furthermore:

- using the assisting approach, ENISA can give support in terms of expertise to the Western Balkans as a region and/or single countries of the region and to countries belonging to the European Eastern Partnership as a region and/or single countries of the region;

- using the outreach approach, and with the endorsement of the Management Board, ENISA can cooperate with third countries with which there are specific EU agreements to enhance mutual cybersecurity awareness and education in line with the respective specific provisions of such agreements.

4.2 STRATEGIC OBJECTIVE 'CYBERSECURITY AS AN INTEGRAL PART OF EU POLICIES'

ENISA collects and exchanges information on best practices in cybersecurity policy development and implementation internationally and promotes the projection of EU cybersecurity policies to the benefit of the Union. ENISA's connections with international organisations working on digital security can both contribute to the promotion of EU acquis in this field and feed into EU cybersecurity policy development. Furthermore:

- using the assisting approach, ENISA can support Union representatives of relevant international organisations and regulatory forums by providing expertise on cybersecurity policies and cybersecurity aspects of Union legislation as outlined under Article 5 of the CSA;

- using the assisting approach, ENISA can provide expertise on cybersecurity policy implementation to the Western Balkans and Eastern Partnership countries;

- using the outreach approach, ENISA can cooperate with the OECD (and like-minded countries such as the Unites States) on mapping and promoting best practices in integrating cybersecurity into various policy domains.

4.3 STRATEGIC OBJECTIVE 'EFFECTIVE COOPERATION AMONG OPERATIONAL ACTORS WITHIN THE UNION IN CASE OF MASSIVE CYBER INCIDENTS'

ENISA's international cooperation should assist and contribute to the Union's incident response and crisis management, in particular by building a trusted network of like-minded international partners – including major global cybersecurity companies and vendors – to contribute to the Union's common situational awareness and preparedness. Furthermore, ENISA – in line with recital 43 of the CSA and using the outreach approach – can contribute to this by cooperating with international partners such as the OSCE and NATO on joint incident response coordination ([5]).

4.4 STRATEGIC OBJECTIVE 'CUTTING-EDGE COMPETENCES AND CAPABILITIES IN CYBERSECURITY ACROSS THE UNION'

ENISA will seek to reach out to international partners to exchange information and best practices in order to enhance and develop cybersecurity competences and capabilities within the Union. Where appropriate, it can participate as an observer in the organisation of international cybersecurity exercises in line with Article 12 of the CSA. Furthermore:

- using the assisting approach, ENISA can contribute to building competences and capabilities in the Western Balkans as a region and/or single countries by supporting training and exercises;

- using the assisting approach, ENISA can support, with relevant expertise, countries belonging to the Eastern Partnership as a region and/or single countries of the region or countries benefiting from the Union's development programmes;

- in line with recital 43 of the CSA and using the assisting approach, ENISA can contribute to the organisation of joint cybersecurity exercises with the OECD, the OSCE and NATO;

- under the outreach approach, ENISA can organise international cybersecurity challenges to promote and enhance the competitiveness of cybersecurity competences in the Union;

[5] Those activities are to be carried out in full respect of the principles of inclusiveness, reciprocity and the decision-making autonomy of the Union, without prejudice to the specific character of the security and defence policy of any Member State.

- using the outreach approach, and with the endorsement of the Management Board, ENISA can cooperate with third countries with which there are specific EU agreements to build and enhance mutual cybersecurity capacities in line with the respective specific provisions of such agreements.

4.5 STRATEGIC OBJECTIVE 'A HIGH LEVEL OF TRUST IN SECURE DIGITAL SOLUTIONS'

Without prejudice to possible tasks stemming from Article 12(d) of the CSA, ENISA will seek to advance its expertise and monitor international developments in cybersecurity certification and related standardisation areas, also in line with Article 54 of the CSA ([6]). It will engage with international actors on the supply and demand sides of the cybersecurity market to promote and advance European digital autonomy. Furthermore:

- using the outreach approach, ENISA will engage with the relevant key strategic economic partners of the Union to promote the EU's cybersecurity certification schemes or candidate schemes;

- using the outreach approach, and in line with recital 23 of the CSA, ENISA will support the global development and maintenance of standards that underpin the public core of the open internet and the stability and security of its functioning.

4.6 STRATEGIC OBJECTIVE 'FORESIGHT ON EMERGING AND FUTURE CYBERSECURITY CHALLENGES'

ENISA aims to exchange information on an ad hoc basis and participate in international forums to increase its expertise in international developments and map global cybersecurity threats as well as research areas and innovation trends that could address emerging challenges.

4.7 STRATEGIC OBJECTIVE 'EFFICIENT AND EFFECTIVE CYBERSECURITY INFORMATION AND KNOWLEDGE MANAGEMENT FOR EUROPE'

ENISA aims to gain a better overview and understanding of the international cybersecurity landscape and ensure that relevant cybersecurity information and knowledge generated internationally is shared and expanded within the EU cybersecurity ecosystem. ENISA will focus its outreach to partners deemed like-minded (e.g. Japan). Furthermore:

- using the outreach approach, ENISA will cooperate with the OECD and NATO in exchanging expertise for the development of cybersecurity indices and benchmarks;

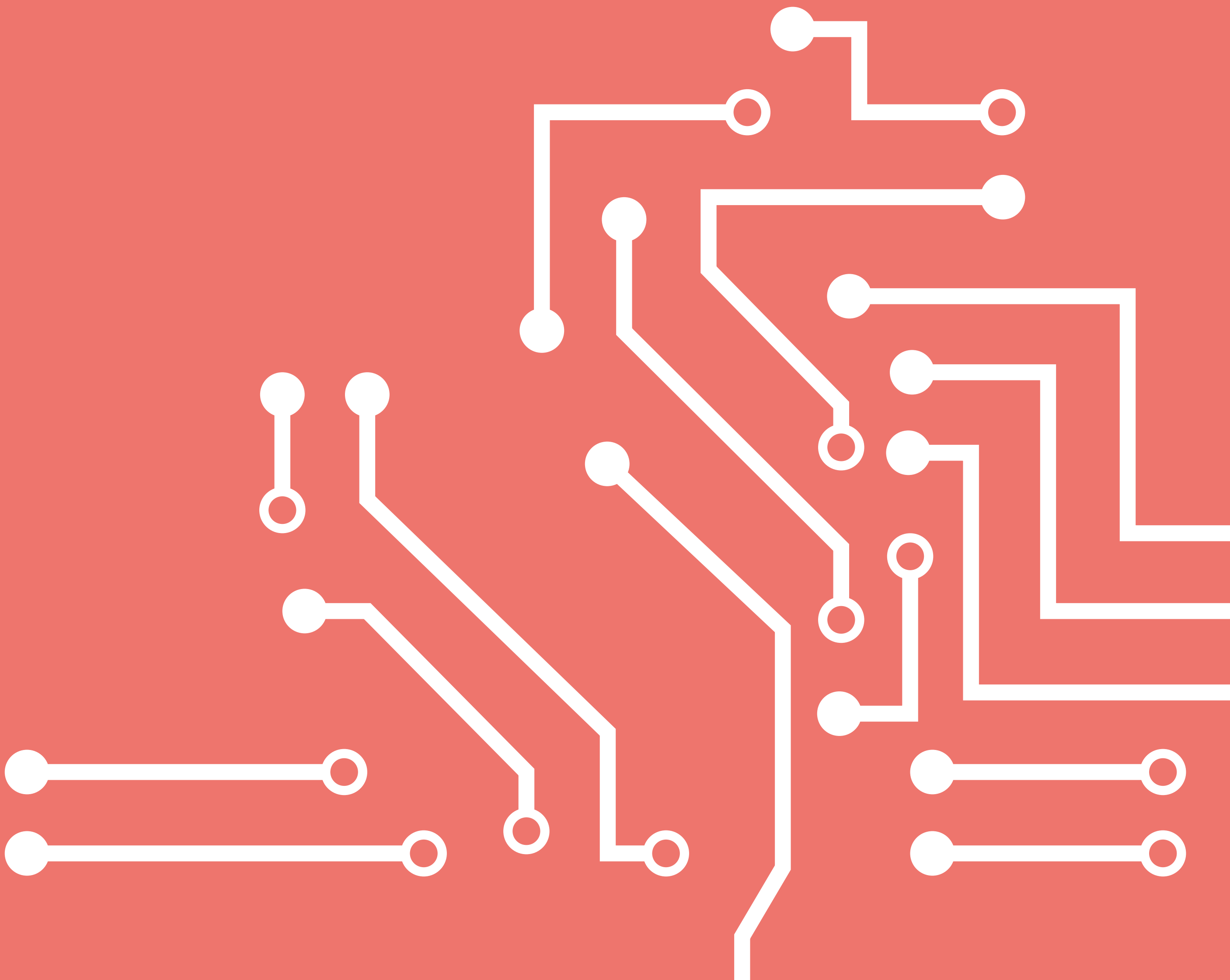
- using the outreach approach, and with the endorsement of the Management Board, ENISA will cooperate with third countries with which there are specific EU agreements to enhance mutual knowledge and information in line with the respective specific provisions of such agreements.

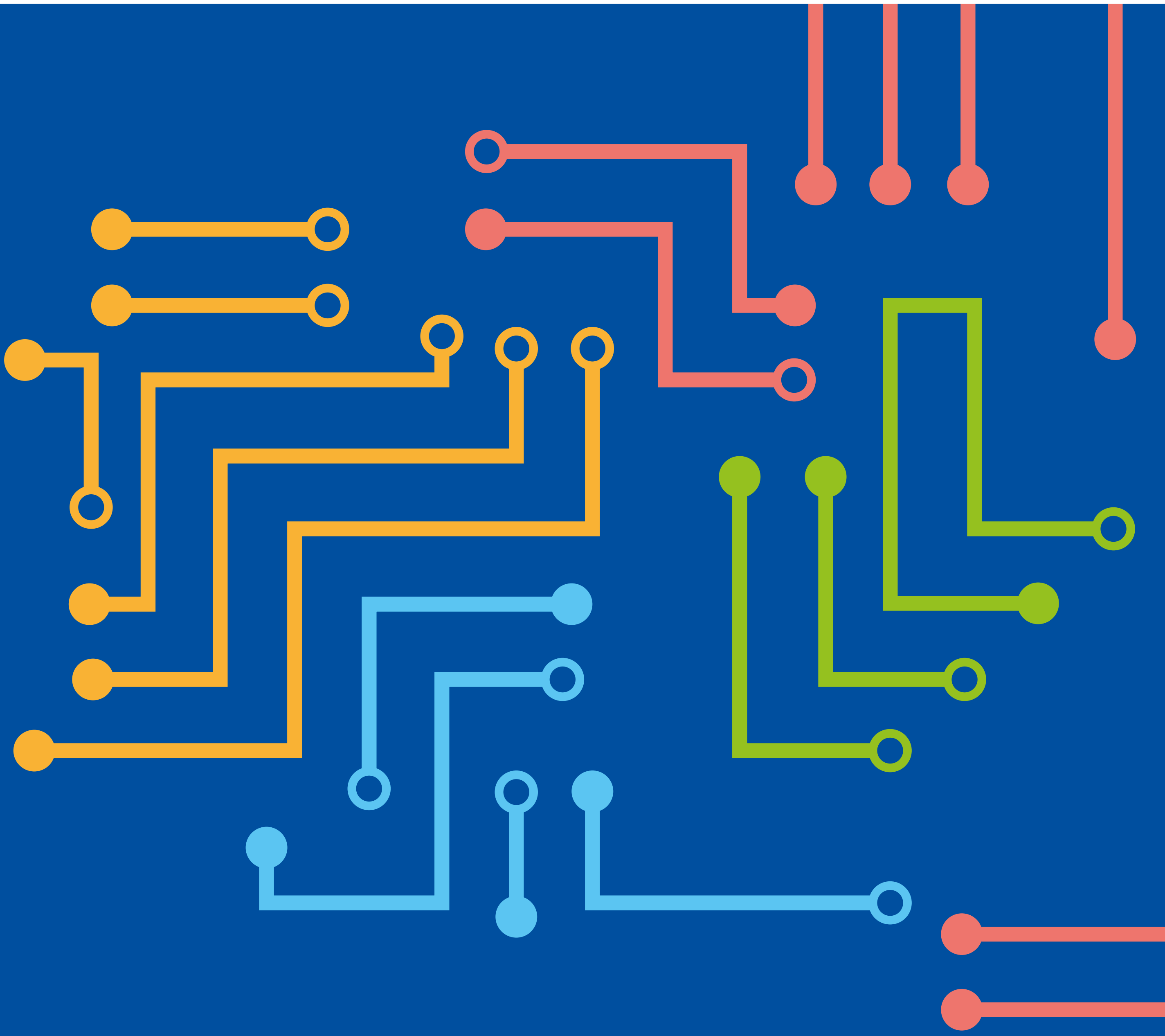
[6] Article 54 (elements of European cybersecurity certification schemes) of the CSA states that 'A European cybersecurity certification scheme shall include at least the following elements: […] (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme; […] (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services and ICT processes, security requirements, evaluation criteria and methods, and assurance levels.'

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**.

Print	ISBN 978-92-9204-565-4	doi: 10.2824/597708	TP-09-22-074-EN-C
PDF	ISBN 978-92-9204-564-7	doi: 10.2824/145196	TP-09-22-074-EN-N





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

Publications Office
of the European Union