



EUROPEAN UNION AGENCY FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

ENISA Strategy

June 2020



A TRUSTED
AND CYBER SECURE
EUROPE

EUROPEAN UNION AGENCY FOR CYBERSECURITY



FOREWORD

For more than 15 years, ENISA – the EU Agency for Cybersecurity – has played a key role in enabling the EU’s ambition to reinforce digital trust and security across Europe, together with the Member States and EU Institutions and Agencies. By bringing communities together, ENISA successfully contributed to strengthening Europe’s preparedness and response capabilities to cyber incidents.

Simultaneously, the digitalisation of our economy and society has drastically increased, as demonstrated during the COVID-19 crisis when a collective and massive turn to remote IT solutions was essential to keep many activities going. This crisis outlined how much cyber attackers take advantage of our dependency on these technologies. It also revealed how the cyber threat landscape has broadened from targeted attacks to new forms of massive threats to millions of businesses and citizens including a rising number of sophisticated ransomware incidents. The rapid development of digital products and services, from Cloud and videoconferencing to 5G and A.I., also brought new challenges to uncover and address.

With its permanent mandate and enhanced tasks and capabilities, ENISA is, more than ever, meant to play a leading role in helping the EU and its Member States keep up with these challenges, while a new era dawns for cybersecurity in Europe.

To do so, ENISA will work towards anticipating relevant trends, pull and share state-of-the-art expertise

and knowledge for all. It will support the European Commission and the Member States in helping public and private actors and citizens to prevent and manage risks associated with cyber incidents. With the implementation of the cybersecurity certification framework, ENISA will contribute to a paradigm shift by improving the level of security of digital solutions deployed in Europe. In doing so, it will increase the ability of all to choose and trust. The Agency will also actively support the European cybersecurity operational community in closely cooperating and preparing to respond together when the next large-scale cyber incident hits Europe.

As ENISA takes up its new role, openness, agility and reliability will be key drivers in its daily operations, while working closer with the Member States and the European Commission in aligning approaches. ENISA will also strive to improve its environmental impact in the context of the ongoing climate crisis and to be a socially responsible and inclusive working environment.

This Strategy document, developed through the engagement of all of ENISA’s staff, the members of its Management Board and its Advisory Group in a collaborative and inclusive process, sets the clear objectives that will drive ENISA’s work in the coming years to meet the many challenges ahead.

On behalf of the Management Board

Jean-Baptiste Demaison

Chair of the Management Board

Krzysztof Silicki

Deputy Chair of the Management Board

VISION

A trusted and cyber secure Europe

MISSION

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.

VALUES

Community Mind-Set

ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence

ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

Integrity/ethics

ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect

ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

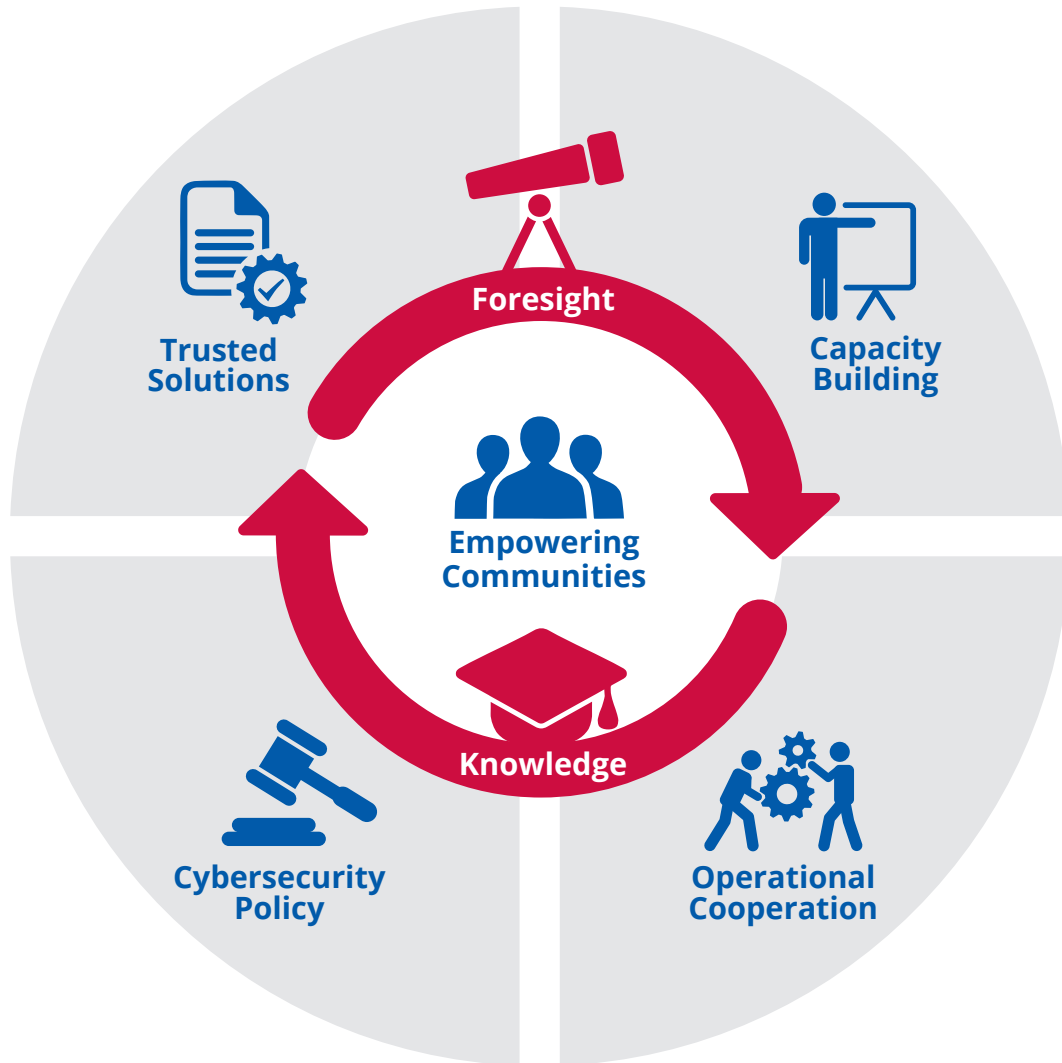
Responsibility

ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency

ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

STRATEGIC OBJECTIVES



SO1

Strategic objective



EMPOWERED AND ENGAGED COMMUNITIES ACROSS THE CYBERSECURITY ECOSYSTEM

Context

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

What we want to achieve

- An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies.
- An empowered cyber ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure;



SO2

Strategic objective



CYBERSECURITY AS AN INTEGRAL PART OF EU POLICIES

Context

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must therefore be embedded across all domains of EU policy. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

What we want to achieve

- Proactive advice and support to all relevant EU-level actors bringing in the cybersecurity dimension in policy development lifecycle through viable and targeted technical guidelines;
- Cybersecurity risk management frameworks that are in place across all sectors and followed throughout the cybersecurity policy lifecycle.

S03

Strategic objective




EFFECTIVE COOPERATION AMONGST OPERATIONAL ACTORS WITHIN THE UNION IN CASE OF MASSIVE CYBER INCIDENTS

Context

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

What we want to achieve

- Continuous cross-border and cross layer support to cooperation between Member States as well as with EU institutions. In particular in view of potential large scale incidents and crises, support the scaling up of technical operational, political and strategic cooperation amongst key operational actors to enable timely response, information sharing, situational awareness and crises communication across the Union;
- Comprehensive and rapid technical handling upon request of the Member States to facilitate technical and operational needs in incident and crises management.

The background features a vertical gradient from light orange at the top to a darker orange at the bottom. Scattered across this gradient are numerous small, semi-transparent yellow dots of varying sizes, creating a starry or confetti-like effect.

SO4

Strategic objective



CUTTING-EDGE COMPETENCES AND CAPABILITIES IN CYBERSECURITY ACROSS THE UNION

Context

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

What we want to achieve

- Aligned cybersecurity competencies, professional experience and education structures to meet the constantly increasing needs for cybersecurity knowledge and competences in the EU;
- An elevated base-level of cybersecurity awareness and competences across the EU while mainstreaming cyber into new disciplines;
- Well prepared and tested capabilities with the appropriate capacity to deal with the evolving threat environment across the EU.

S05

Strategic objective




HIGH LEVEL OF TRUST IN SECURE DIGITAL SOLUTIONS

Context

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

What we want to achieve

- Cyber secure digital environment across the EU, where citizens can trust ICT products, services and processes through the deployment of certification schemes in key technological areas;



S06

Strategic objective



FORESIGHT ON EMERGING AND FUTURE CYBERSECURITY CHALLENGES

Context

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

What we want to achieve

- Understanding emerging trends and patterns using foresight and future scenarios that contribute to mitigating our stakeholder's cyber challenges;
- Early assessment of challenges and risks from the adoption of and adaptation to the emerging future options, while collaborating with stakeholders on appropriate mitigation strategies.



SO7

Strategic objective



EFFICIENT AND EFFECTIVE CYBERSECURITY INFORMATION AND KNOWLEDGE MANAGEMENT FOR EUROPE

Context

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

What we want to achieve

- Shared information and knowledge management for the EU cybersecurity ecosystem in an accessible, customised, timely and applicable form, with appropriate methodology, infrastructures and tools, coupled and quality assurance methods to achieve continuous improvement of services.



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 on www.enisa.europa.eu



ENISA

European Union Agency for Cybersecurity

Athens Office

1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

