

Cyber Security Beyond 2020

Paulo Empadinhas | Steve Purser

NLO meeting | ENISA Athens | 26/04/2017

Main findings

ENISA's current tasks and product portfolio shall be retained.

A number of existing tasks and service offerings need to be reinforced, and several new tasks and orientations should to be considered. The complete security life cycle shall be addressed in this approach.

ENISA shall have the power to act on its own initiative and to engage in the complete security life cycle.

The future mandate should be scoped more broadly to allow for a coherent approach to EU cyber security and give greater consideration to the economic and societal aspects of cyber security where ENISA could also play a role.

In scoping ENISA's role and tasks, it would be important to define clearly the scope of different other actors in the EU cyber security space.

A new governance structure along the lines being considered by other agencies could be suggested to improve the decision-making process.

Role/responsibilities for ENISA
Key elements of a future **permanent** mandate for ENISA

Policy advice: provision of strategic policy advice to the EU institutions and MS in relation to cyber security.

Information and **capability-building**: ENISA as the EU Cyber security Information Hub offering high quality cyber security analysis and training.

Cyber security lifecycle: getting more involved in the complete cyber security lifecycle, including practical, "hands-on" support and an incident response (coordination) capacity.

Trends: ENISA using its unique cyber security knowledge to identify trends and forecasting threats and potential solutions.

Collaboration: providing and maintaining an expert infrastructure platform connecting all players EU-wide and beyond.

Research: contributing to the EU cyber security research agenda and supporting the development of research results in a commercial environment.

Industry: strengthen the engagement the private sector, for instance by involving the industry in the governance of ENISA.

Standards and certification: ENISA developing and promoting cyber security standards, managing certifications.

Alternative business models: exploring the possibility of creating revenue, including providing remuneration services e.g. by way of SLAs with EU institutions and agencies, and industry.

The current mandate is refected in the ENISA strategy

#Expertise **Anticipate and support Europe in facing emerging network and information security challenges**, by collating, analyzing and making available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment.

#Policy **Promote network and information security as an EU policy priority**, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.

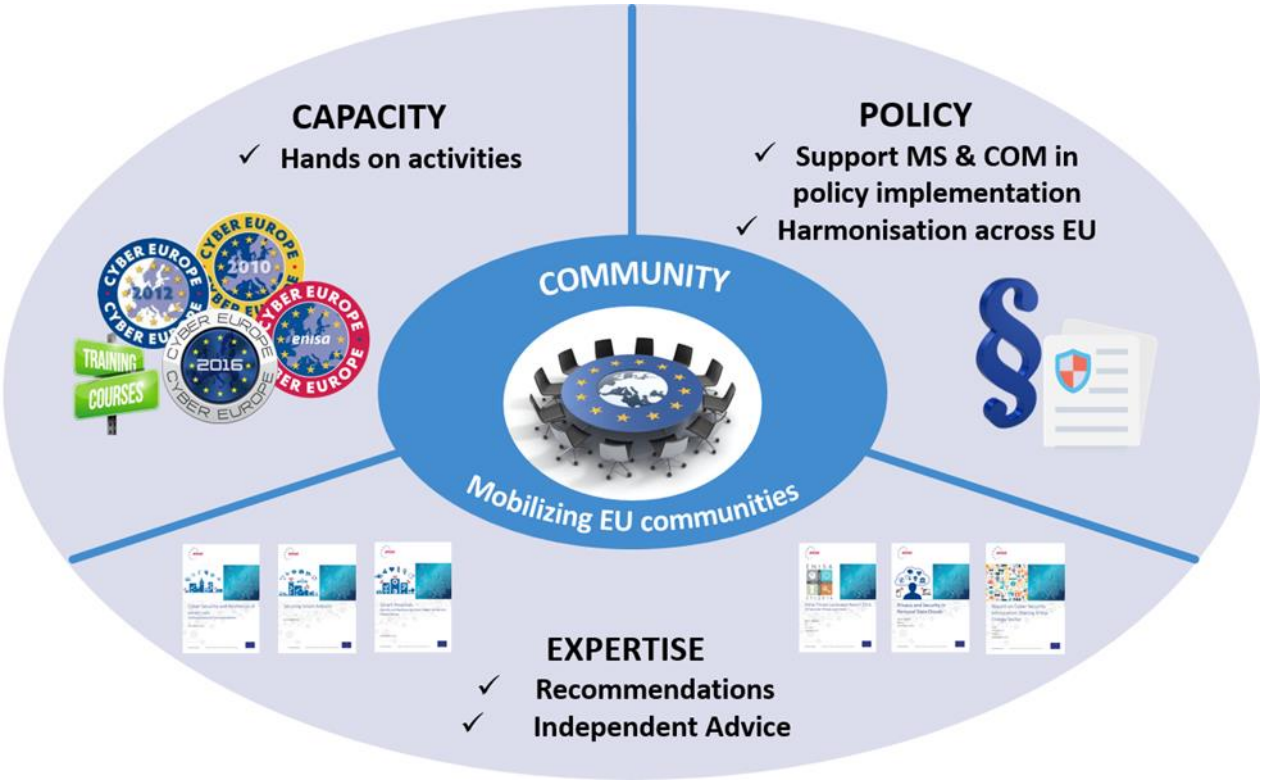
#Capacity **Support Europe maintaining state-of-the-art network and information security capacities**, by assisting the Member States and European Union bodies in reinforcing their NIS capacities.

#Community **Foster the emerging European network and information security community,** by reinforcing cooperation at EU level among Member States, European Union bodies and **relevant** NIS stakeholders, including the private sector.

One horizontal objective complements the above and is described here.

#Enabling **Reinforce ENISA's impact**, by improving the management of its resources and engaging more efficiently with its stakeholders, including Member States and Union Institutions, as well as at international level.

Current 4 Core Objectives



Overall, all current agency tasks are relevant and should be maintained.

In terms of new ideas for tasks, the following have been put forward for consideration:

- Coordinating network information security and cyber security activities and response at EU level (ENISA as the EU *Single Point Of Contact* (SPOC) for cyber security incident response);
- Supporting the development of EU minimum standards on cyber security;
- Working with the EU Commission, having a better-defined role in research, including:
  - setting priorities for research in cyber security (policy and industry needs);
  - helping to transition cyber security research into the market place;
- Providing the EU Cyber security Information Hub;
- Establishing with industry a Cyber security Training Centre;
- Assessing awareness needs across EU-28, advise on “gaps”, providing awareness material, coordinating awareness campaigns across the EU;

Overall, all current agency tasks are relevant and should be maintained.

- Serving as the EU interface to bodies that are part of global cyber security response;
- Giving National Liaison Officers (NLOs) a statutory basis;
- Formalising and making more specific the process of receiving external funding, e.g. working with purchase orders with clearly defined scope and expected results;
- Analysing the economic and societal aspects and implications of cyber security (e.g. economic analysis);
- Formalising ENISA's role in supporting the implementation of GDPR;
- In conjunction with the EEAS, having specific powers to assist third countries with tasks falling within the ENISA mandate;
- Alternative funding mechanisms:
  - ENISA providing specific consultancy services for public bodies on a cost recovery basis;
  - ENISA being able to apply for/benefit from research funding.

Emerging strategic themes 1/7

A comprehensive mandate allowing for a coherent approach to EU cyber security

- Agility in delivering added value in a constantly changing landscape
- Supporting the development and implementation of EU cyber policy and strategies
- Mandate should address issues and opportunities for both business and technology at EU and possibly international level
- ENISA should be able to act on its own initiative
- ENISA to support the development and implementation of foreign security and defence policies, working closely with the EEAS

Need for a permanent mandate

- ENISA must have a permanent mandate, not simply another extension for a limited number of years
- Adequate resources so that ENISA is not forced to prioritise important cyber activities

Economics of cybersecurity

- Including better engagement with industry to leverage economic opportunities in the EU from cybersecurity

Emerging strategic themes 2/7

Need for a clear definition of the scope and coordination roles of different actors in cyber security

- Many different stakeholders (law enforcement, defence, intelligence, privacy, technological, etc.) should work together in a pre-defined structured way
- The challenge of a multitude of EU and international agencies and complex regulatory landscape needs to be addressed
- ENISA's central role as the internal market agency for cyber security needs to be more explicit

ENISA as the EU Cyber security Information Hub

- Enhancing ENISA's information position by using information available from all stakeholders
- ENISA's added value is high quality analysis and not processing raw data
- Performing strategic analysis and analysis of incidents
- Having an education/training component (Cyber security Training Centre)

Emerging strategic themes 3/7

Involvement at all stages of the cyber security life cycle (Prevent – Detect – Respond)

- Following up on recommendations and good practices to achieve tangible impact
- Moving from “hands off” design role to a more “hands on” implementation role
- Learning from this, using it to enrich the agency’s experience and feeding it back into ENISA’s way of working to improve the quality of service
- Making a “hands on” rather than theoretical contribution to the EU cyber security debate
- Developing a response capacity to cyber security incidents, coupled with crisis management to complement at EU level the MS effort in this area

ENISA as a contributor to the coordination of cyber security incident response in the EU

- Coordinating network information security and cyber security incident response at EU level
  (ENISA as the EU SPOC (Single Point of Contact) for cyber security incident response)
- Physical presence (on-the-spot), supporting a SPOC, disseminating remediation or threat insights, in response to large-scale or critical infrastructure incidents

Emerging strategic themes 4/7

Using ENISA's enhanced cyber security information positon to identify trends, threats and responses

- Anticipating challenges and risks, emerging threats, technology developments
- Early warning services and strategic analysis
- Offering insight into the "next big thing", e.g. black swans

Supporting the development of and promoting cyber security standards

- Identifying standardisation gaps, working with all actors to identify strategic roadmaps and oversee standardisation activities
- Using ENISA good practices as standards precursors
- Ensuring different stakeholders' perspectives (including industry/private sector) are taken into consideration throughout the standardisation process
- Involvement in setting EU minimum standards on cyber security on the basis of trends and needs

Maintaining and managing cyber security certifications

- Supporting the writing of certifications and reflecting changes based on technology or threat evolution

Emerging strategic themes 5/7

ENISA supporting standardisation and certification

- Support accreditation/standardisation activities
- Being active in accreditation
- A role for ENISA in cyber security certification – complementing national certifications with an EU one

Providing and maintaining an expert infrastructure platform e.g. Connected European Facilities SMART connecting all players EU-wide and beyond

- Mobilising expert networks, serving as a driver/champion
- Operating the associated infrastructure
- Consider offering new means/ways to collaborate
- Continued focus on common effort, support, connecting the dots
- Serving as an interface to institutions that are part of global cyber security response
- Having specific powers to assist third countries with tasks falling within the ENISA mandate

Emerging strategic themes 6/7

Better engaging industry/the private sector

- Involving the private sector in the governance of ENISA (e.g. stronger role of Permanent Stakeholders' Group and a different composition of the Management Board to include representatives of industry)
- ENISA's position as an independent advisor to be maintained

Bridging the gap between cyber security research results and the market

- Better use of research results
- No institution tasked with the responsibility to support the development of research results in a commercial environment
- ENISA to nurture cyber security research and help with commercialisation
- In addition, there could be a role for ENISA in channelling/promoting and disseminating cyber security research results across Member States and industry

Contributing to the EU cyber security research agenda

- ENISA could contribute to cyber security research priority-setting (e.g. "EU Commission to take utmost account of ENISA recommendations on cyber security" on this)

Emerging strategic themes 7/7

Pragmatic involvement in policy advice

- ENISA to provide: (i) analysis on trends and threats, (ii) opinions, (iii) recommendations and to (iv) address future challenges not yet identified

Greater consideration of the economic and societal aspects of cyber security

- Looking into the societal and economic dimension of cyber security which is currently not being adequately addressed by ENISA
- Given that ENISA is a single market agency, it could consider developing a level of economic analysis in relation to cyber security in the EU
- This would help ensure that cyber security is an economic enabler and not a barrier to the delivery of the digital economy

Exploring the possibilities of providing remunerated services and other alternative business models by way of SLAs with EU institutions and agencies and industry

- Regarding governance arrangements:
  - retain Permanent Stakeholders' Group (PSG)
  - consider, in line with other EU agencies, an alternative governance structure for the agency, in order to improve efficiency of the decision-making process (NLO, PSG, Executive Board, Management Board (MB)).

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu