ENISA'S INPUT TO THE MANDATE RENEWAL DISCUSSION

The EU Cyber Security Agency

ENISA.EUROPA.EU

ENISA - a strong partner in securing Europe's cyberspace

VERSION B| JULY 2017

Foreword from the Executive Director

Let us step back in time to Friday October 21, 2016, after 11:10 UTC. If you typed the URL of some well-known US internet service providers into your browser there was no response[1], and no online services available. The reason - the Mirai botnet[2] had hacked millions of Internet-Of-Things devices and collectively performed a Denial-Of-Service attack on a Domain-Name-Service provider with the result that the IP-addresses of hundreds of company services could not be accessed anymore. It was like removing the telephone number of these organisations in a way that customers could not contact them.

Estonia 2007[3], Georgia 2008[4], Iran (Stuxnet) 2010[5], the Snowden[6] revelations of 2013, the scandal of hacked emails[7] in US election in 2016 are only a few examples of the new virtual Wild West in cyber space.

In the past, one needed a gun to rob a bank, today an equivalent amount of damage can be achieved from the action of a fingertip on a keyboard. This exercise can be performed from any place in the world. Crime, espionage, sabotage and even international conflicts move from the so-called real world into the virtual cyber world. On top of this, the terrorists' attacks in Brussels and Berlin last year resulted in a new debate on the use of cryptography[8] linked to criminal justice in cyber space[9].

Are we prepared to address the real challenge arising from new threats and the new hybrid threat landscape? Yes and No. This question does not have a straight answer.

In 2009, the European Commission published the Communication on Critical Information Infrastructure Protection (CIIP) [10]. In the following years, COM launched several strategies: the EU Cybersecurity strategy in 2013[11], the European Agenda on Security in 2015[12], (where cyber issues are mentioned, including fighting cyber crime however, ENISA is not mentioned) and the Digital Marketing Strategy[13].

[1] 2016 cyberattack, available at: https://en.m.wikipedia.org/wiki/2016_Dyn_cyberattack
[2] Dyn Analysis Summary Of Friday October 21 Attack, October 26th, 2016, available at: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[3] 2007 cyberattacks on Estonia, available at: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[4] Cyberattacks during the Russo-Georgian War, available at: https://en.m.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War
[5] Stuxnet, computer worm, discovered in June 2010, available at: https://en.m.wikipedia.org/wiki/Stuxnet
[6] Edward Snowden, American whistleblower and former National Security Agency contractor, available at: https://en.m.wikipedia.org/wiki/Edward_Snowden
[7] Hillary Clinton Email Archive on WikiLeaks, available at: https://wikileaks.org/clinton-emails/emailid/30373
[8] Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, November 2016, Presidency progress report no. 14711/16, available at: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf
[9] Outcome of the 3508th Council meeting on Justice and Home Affairs, 15391/16, December 2016, page 7, available at: http://www.consilium.europa.eu/en/meetings/jha/2016/12/st15391_en16_pdf/
[10] COM Communication on CIIP, COM(2009) 149 final, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[11] Cybersecurity Strategy of the EU (2013), JOIN (2013) 1 final, – see Annex B.
[12] The European Agenda on Security (2015), COM/2015/0185 final, – see Annex B.
[13] Digital Single Market Strategy for Europe (DSM) (2015), COM/2015/0192 final, – see Annex B.

Furthermore, in 2016, a Joint Framework on countering hybrid threats[14] was published and the cPPP initiative[15] was launched. The European Parliament and Council adopted in 2016 the General Data Protection Regulation (GDPR)[16], Law Enforcement Authorities (LEA) data protection Directive[17], the Passenger Name Records Directive[18] and the NIS directive[19]. These initiatives demonstrate that political awareness results in political action.

On the implementation side, ENISA was established in 2004 to support the security of network and information systems across the EU, and its mandate was renewed in 2009 and 2013[20]. Even with its limited resources, of about €11 Million /year, ENISA has published and covered nearly every upcoming topic relevant for cybersecurity and cyber space. Examples of published reports include ENISA Threat Landscape, activities on exercises, reports on Smart Airports, Smart cities, eHealth, to name a few[21].

However, this is not enough!

If someone looks into the evolution of information technology and computer science, the last decades were governed by Moore's law, i.e. more and more computer power, scalable availability everywhere (i.e. cloud computing), and easy to use devices (i.e. smartphones). These technologies have challenged traditional business models and have resulted in the concept of disruptive technologies. Nevertheless, with the latest discussions that the US presidential elections were influenced by state actors[22] and the fear that the upcoming French, German and Dutch elections[23] [24] [25] could be manipulated, cybersecurity is also now seen as global political challenge.

EU bodies and institutions should work in a harmonized manner, to address the challenges and opportunities of cybersecurity. While this topic is generally driven from an infrastructure perspective, it is currently becoming a topic of foreign and security policy.

Existing institutions, like ENISA, should be strengthened and their role expanded to leverage their technical expertise in NIS, their ability to cooperate with EU institutions and bodies and with MS national authorities on NIS topics, as well as on data protection and cybercrime.

The geopolitical challenges should be considered when assessing the EU cybersecurity architecture, when clarifying the roles and responsibilities in all the security lifecycle steps ranging from protection, prevention to mitigation and response/defence in reaction to cyber incidents. In this regard, ENISA needs to support

---

[14] Joint Communication on countering hybrid threats (2016), JOIN/2016/018 final, – see Annex B.
[15] See COM communication 0410/2016 on cPPP (Cybersecurity Public-Private partnership) (2016) and COM decision C(2016)4400 on cPPP (2016) in Annex B.
[16] General Data Protection Regulation (2016) (GDPR), Regulation (EU) 2016/679, – see Annex B.
[17] LEA Data protection Directive (2016), Directive (2016) (EU) 2016/680, – see Annex B.
[18] PNR (passenger name record) Directive (2016), Directive (EU) 2016/681, – see Annex B.
[19] The NIS Directive, Directive (EU) 2016/1148, – see Annex B.
[20] ENISA Regulation (2013), Regulation (EU) No 526/2013, – see Annex B.
[21] ENISA publications available at: https://www.enisa.europa.eu/publications
[22] US intelligence report: Vladimir Putin 'ordered' operation to get Trump elected, The Guardian, available at: https://www.theguardian.com/world/2017/jan/06/vladimir-putin-us-election-interference-report-donald-trump
[23] Russian cyber-attacks could influence German election, says Merkel, The Guardian, available at: https://www.theguardian.com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel
[24] France's Hollande seeks 'specific measures' against election hacking, Politico, 15/02/2017, available at: http://www.politico.eu/article/frances-hollande-seeks-specific-measures-against-election-hacking-russia-putin/
[25] Dutch will count all election ballots by hand to thwart hacking, The Guardian, available at: https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking

the EU foreign security and defence policy. To face the technological, geopolitical and economic challenges in the EU, two essential things need to be addressed:

1. The EU Commission, together with the MSs, to examine and adjust where necessary the current European governance structure regarding ICT and cybersecurity,
2. Significantly strengthen the mandate of ENISA, especially to give ENISA a stronger position in addressing the cybersecurity lifecycle challenges and improving the ability to address its own initiative tasks list. It is acknowledged that this will require an increase in its budget.

The current evaluation of ENISA and the envisaged new ENISA mandate proposal of the Commission is a unique opportunity to address the challenges mentioned above.

This document is intended to support and foster the discussions on ENISA's mandate. It summarises the current landscape and raises topics and ideas for the future and a stronger mandate for ENISA. The target audience of this document are primarily the political decision makers in Brussels (the Commission, the EU Parliament, and the Council) and the representatives of the member states. The target audience also includes our stakeholders in industry and academia. We welcome input and discussion from all. It is hoped that the forthcoming discussions on the future of ENISA will well position the agency to meet the challenges of the cyber space of the future.

The main areas in which ENISA believes its mandate should be expended are as follows:

1. **Organic growth**: continuing the evolution of the functions of the Agency to address the latest cybersecurity challenges including ***reinforcing the role in securing CIIP.***

2. **Policy advice**: provision of strategic policy advice to the EU institutions and MS in relation to cybersecurity; ENISA should also be in a position to produce its own initiative policy advice. This includes:
   Aligning cybersecurity research with policy & commercialisation,
   Addressing cybersecurity policy fragmentation,
   Involvement in all key policy initiatives.

3. **Information** and **capability building**: ENISA as the EU Cybersecurity Information/***coordination*** Hub offering high quality cybersecurity analysis and training and strengthens ENISA's role as a single point of contact in the area of ***cyber crisis cooperation / technical support***.

4. ***Cybersecurity lifecycle***: getting more involved in the complete cybersecurity lifecycle, including practical, "hands-on" support and an incident response (coordination) capacity,

5. ***Economics of cybersecurity***: including better engagement with industry to leverage economic opportunities in the EU from cybersecurity,

6. **Standards and certification**: ENISA developing and promoting ***cybersecurity standards process***, managing ***ICT security certifications***.

7. ***Coverage of geopolitical and societal developments.*** This is a logical extension of the work that ENISA is doing in the area of threat analysis and will provide stakeholders with a more complete picture of the cybersecurity landscape. In addition, ENISA should be involved in ***increased international cooperation.***

I believe that Europe needs a strong cybersecurity agency that addresses the needs and challenges of information and network security. ENISA is well placed and has the experience of collaborating with the key stakeholders at Member State and at EU level in this area.

Our political leaders are committed to building the future wealth of the EU by leveraging the opportunities of the Digital Society. The security of cyber space is particularly important where we use technology that ignores the traditional boundaries of distance and borders. Cybersecurity is an integral part and extends from the personal use of ICT to the most complex industrial control systems and critical infrastructures. New technologies are quickly finding new applications that affect our everyday lives.

ENISA is already working in all these areas, is contributing to the advancing of European network and information security, and will continue to do so if the necessary resources are put in place.

ENISA has contributed to the EU cybersecurity landscape since 2004. ENISA is addressing and will continue to address the cybersecurity challenges, to support the political goal of harnessing the opportunities of the Digital Society. ENISA's role needs to be further developed and strengthened to adequately contribute to the EU cybersecurity world post 2020.

It is against this background I present our vision for a stronger European cybersecurity Agency that will meet the cybersecurity challenges of the future.

Udo Helmbrecht

Contents

1. Introduction

The mandate of the European Union Agency for Network and Information Security (ENISA) expires on 18th of June 2020. The renewal of the mandate will require the bringing forward of a proposal by COM[26] [27]and the agreement of the Council and the Parliament.

The continually changing cybersecurity threat landscape[28] and the evolution of related European Union (EU) policy necessitate a critical look at ENISA's mandate and tasks.

Given the length of time to bring forward and have adopted EU legislation, discussions are already taking place on the renewal of the mandate. The mandate of ENISA was renewed in 2009 and 2013. Given the increasing recognition of the importance of cybersecurity the mandate has evolved and an increasing amount of functions are being assigned to ENISA by way different pieces of legislation. The most recent and important tasks for ENISA have emerged from the Adoption of the NIS Directive in 2016 where ENISA was tasked with functions to support the CSIRT network and the Cooperation group.

In the pursuit of an open, safe and secure cyber space, ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA also supports the development and implementation of European Union policy and law on matters relating to network and information security (NIS). ENISA is the European cybersecurity agency, which determines and addresses network and information security issues, thereby contributing to the proper functioning of the internal market. It also aims to exploit the full potential of the internal market from the widespread use of information and communications technologies (ICT) in a safe and secure cyber space. While ICT technologies present business opportunities in cyber space they also present opportunities for crime and misuse, which need to be considered and addressed.

This document presents a number of strategic themes to be considered in upcoming reflections on the ENISA mandate and can serve as a basis for discussions as it presents the agency's position in further mandate negotiations.

In Section 2, the current context is described including some of the challenges in securing the cyber space.

In Section 3, the current legal basis of ENISA and its evolution as well as the agency's strategy are introduced. Besides these, an analysis is presented regarding the drivers for change and analysis of current tasks and emerging topics. This section lists several strategic themes and additional considerations that are expected to guide changes to the current mandate.

Section 4 contains ENISA's vision for the future. It includes opinions on evolution of ENISA and ENISA's role in the EU cybersecurity governance. Furthermore, the section includes description of proposed new areas to be covered by a renewed ENISA mandate, including a mapping of the proposed new tasks into current ENISA strategy.

---

[26] Article 32 of ENISA regulation (2013) specifies that by 20th of June 2018 the COM shall commission an evaluation. The evaluation shall address the possible need to modify the mandate of the Agency and the financial implications.
[27] COM Work Programme 2017, COM(2016) 710 final, Annex 2, available at https://ec.europa.eu/info/publications/work-programme-commission-key-documents-2017_en
[28] ENISA publications available at: https://www.enisa.europa.eu/topics/threat-risk-management?tab=publications

2. Background

During the past decade new institutions and organisations have been set up across the EU and Member States to address cybersecurity challenges. This area is developing and the roles and responsibilities of the institutions involved are still being determined or clarified.

The *Global Strategy for the European Union* (EUGS)[29], which is the strategy for the EU's foreign and security policy, and provides priorities for a stronger Europe was adopted by the European Foreign Affairs Council on October 2016[30]. The EUGS acknowledges the need for a shared vison to cover priorities such as *Security of the Union* as well as *State and societal resilience*.

Enhanced "*efforts on defence, cyber, counterterrorism, energy and strategic communication*" have also been identified as a *Security of the Union* priority. The need for stakeholders to work closely with their partners, including NATO, has also been highlighted.

In the EUGS it is also mentioned that: "*The EU will increase its focus on cybersecurity, equipping the EU and assisting Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyber space. This entails strengthening the technological capabilities aimed at mitigating threats and the resilience of critical infrastructure, networks and services, and reducing cybercrime. It means fostering innovative information and communication technology (ICT) systems which guarantee the availability and integrity of data, while ensuring security within the European digital space through appropriate policies on the location of data storage and the certification of digital products and services. It requires weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation. The EU will support political, operational and technical cyber cooperation between Member States, notably on analysis and consequence management, and foster shared assessments between EU structures and the relevant institutions in Member States. It will enhance its cybersecurity cooperation with core partners such as the US and NATO. The EU's response will also be embedded in strong public-private partnerships. Cooperation and information-sharing between Member States, institutions, the private sector and civil society can foster a common cybersecurity culture, and raise preparedness for possible cyber disruptions and attacks.*"

In the *State and societal resilience* section of the same EUGS document, it is acknowledged the need for resilience, which is defined therein as "*the ability of states and societies to reform, thus withstanding and recovering from internal and external crises*", to ensure sustainable security. Resilience is considered in a wider aspect, encompassing all individuals and the whole of society. *"A resilient society is considered to be a society that features democracy, trust in institutions, and where sustainable development lies at the heart of a resilient state*."

The EUGS also acknowledges in the last principle – global governance for the 21st Century – that "*Without global norms and the means to enforce them, peace and security, prosperity and democracy – our vital interests – are at risk.*"

[29] Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy, June 2016, available at: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
[30] EU Foreign Ministers adopted common conclusions on implementing the EU Global Strategy, October 2016, available at: https://europa.eu/globalstrategy/en/eu-foreign-ministers-adopted-common-conclusions-implementing-eu-global-strategy

Other COM communications and strategies documents recognise the role of cybersecurity in securing EU's future with specified actions i.e. in fighting cybercrime. For instance, The European Agenda on Security (2015)[31], mentions ENISA as contributor to cybersecurity, "*to the EU's response to cybersecurity issues by working towards a high level of network and information security*" when covering priorities such as 'fighting cybercrime'. The document entitled "*The Joint Framework on countering hybrid threats a European Union response*" (2016)[32] also acknowledges the experience of ENISA, in collaboration with MSs, in setting up security requirements and modalities to notify security incidents and to support convergence of risk management approaches. Furthermore, in the context of ensuring sound financial systems, the COM, in collaboration with ENISA, "*will promote and facilitate threat information-sharing platforms and networks and address factors that hinder the exchange of such information*." The COM Communication entitled *Delivering on European Agenda on Security to fight against terrorism* (2016)[33] has the protection of citizens and critical infrastructures as an objective. Despite ENISA not being mentioned in this COM communication, ENISA is adding value in: Standards, Certification, NISD implementation and Information exchange, etc.

From this short summary, it can be concluded that ENISA is acknowledged as an important stakeholder in the EU cybersecurity governance arena. In addition, it can be noted that not all documents refer to ENISA. This could be due to the complex mapping of roles and responsibilities in the cyber space governance of the EU.

ENISA's role in a renewed EU cybersecurity governance. Since inception of ENISA in 2004, ENISA's mandate has evolved. In 2004, the challenge was seen as a technical challenge addressing information and network security. In 2013, the mandate was widened to include references to cybercrime. In 2017, the natural evolution of the mandate should extend to, inter alia, supporting the European foreign security and defence policy.

The cybersecurity ecosystem is changing, and this requires an assessment and adaptation of roles and responsibilities in the different EU institutions and bodies are engaged in cybersecurity.

In the traditional world, roles and responsibilities have been clearly identified and put in place with the passage of time. However, in cyber space these roles and responsibilities are not so clearly defined. This situation arises from the fact that cyber challenges do not respect traditional geographic and physical boundaries. In addition, the speed at which cybercrime, cyber espionage, cyber sabotage and cyber warfare can take place without any physical presence raises difficulties that could not have been envisaged in the traditional world.

Attribution in virtual world is vastly more complex than it was in the traditional world. Criminals and state actors can easily hide behind many networks in different jurisdictions to a level that prosecuting the criminal to a standard of beyond all reasonable doubt is very rare. Successful attribution may require multi-disciplinary skill sets, cross border cooperation and the support of the diplomatic community to ensure the necessary level of cooperation to meet the challenges of modern crime.

[31] The European Agenda on Security, COM(2015)185 final (2015), – see Annex B.
[32] Framework on countering hybrid threats a European Union response (2016), JOIN/2016/018 final, – see Annex B.
[33] COM Communication delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union (2016), COM(2016) 230 final, April 2016 , – see Annex B.

In 2013, the Cybersecurity Strategy of the EU (2013) included a comprehensive view of different players across three key pillars: network and information security (NIS), law enforcement, and defence. It is obvious that these roles and responsibilities requires an update due to changes in the technical and legal operation of modern cyber space.

On European level, institutions like EUROPOL (EC3), Cert-EU, EDA, EASA, etc. deal with cybersecurity related topics. Each of these institutions and bodies across the EU and in the MS have specific competencies and knowledge bases. This paper does not question their role individually. However, it proposes an approach for building an EU governance map, which would rely on maximizing inter-institutional cooperation, collaboration and teamwork for most of activities linked to awareness building, prevention and preparation and information sharing. Thus, cyber coordination at EU level needs to be enhanced.

Input to EU cybersecurity review process. On May 2017[34], the European Commission announced that the EU Cybersecurity Strategy would be reviewed by September 2017. ENISA prepared an input paper[35], covering the priorities and opportunities identified as relevant for this discussion. The input paper includes also ENISA's vision on the governance model for EU cybersecurity cooperation, providing details on the ENISA possible roles and responsibilities. Some of the ideas presented in the input paper are also shortly covered in the last section of this document.

Defining cybersecurity and clarifying areas of interest. Adding to the complexity of the institutional cyber landscape, as mentioned already, cyber does not yet have clear, unambiguous definitions. To understand the scope and challenges in the cybersecurity domain, one must consider how terminology e.g. cyber space, is defined as well. For this paper, we use the definitions for cyber space and cybersecurity provided/proposed in the Terminology Annex A.

Furthermore, from an operational/preventive perspective, it becomes increasingly difficult to separate cybersecurity from cyber defence and to clarify the meaning of cybercrime, cyber espionage, cyber warfare, cyber sabotage, and cyber terrorism. The classification of a cyber incident may often be decided by subjective criteria such as the perception of the attackers, which may be classified as malicious intent, criminal intent, state actor involvement etc.

As already pointed out before, the attribution of cyber attacks is difficult. Collaboration at global level in all stages from prevention, preparedness, detection, investigation and prosecution of cyber incidents is still to be achieved.

There are still questions to be addressed, arising from the lack of clear/final definitions and the cyber challenges:

- How can the line be drawn between civil and military challenges when the origin and scope of an attack is not easy to identify, for instance while an action cannot yet be defined as i.e. cyberwarfare?
- Where does cyber defence becomes cyber offensive/active defence?
- How to separate cybersecurity from cyber defence for instance during the first stages of prevention, analysis, mitigation etc.?
- How to separate network and information security (NIS) from cybersecurity when aiming to reduce vulnerabilities of networks and systems or when developing prevention measures?

[34] https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
[35] Principles and opportunities for a renewed EU cyber security strategy, ENISA contribution to the Strategy review, 2017, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b

- How to handle cross border aspects/global challenges outside of the legal boundaries of states?
- Who would be mandated to take active measures to remove 'small' vulnerabilities which when used in context of, for example, Mirai attack where thousands of inoffensive IoT devices were aggregated to launch significant cyber-attacks?
- Who should cover the costs of analysis and damage arising of cyber incidents?

Need for cross EU cooperation and collaboration. In case of cross border cyber incidents, cyber investigation would require a mix of skills and participation of different institutions/bodies and collaboration guidelines are required. Inspiration could be aviation investigations processes and procedures. The collaboration mechanisms, parties, roles and responsibilities have to be defined.

Instead of a fragmented view, cross-domain collaboration is needed in all stages: from prevention, preparedness and detection, through investigation, to prosecution of cyber incidents.

At EU level the solutions require a need:

(i) to develop strong institutions specialised in NIS able to collaborate and support national authorities and
(ii) to clarify their roles and interactions in all stages: prevention, preparedness, detection, investigation and prosecution of incidents, as well as having an active defence capability.

Collaboration and cooperation are key, next to existence of an information hub to improve prevention and lessons learned. There is a need for a Neutral independent stakeholder. To improve the level of preparedness it is considered essential to provide this neutral independent stakeholder, with access to data/information, capacity of analysis, capacity to gather skills and expertise from other institutions i.e. for the purpose of and cyber investigation.

The objectives of the neutral independent stakeholder would to

(a) identify causes (using the access to all information),
(b) develop lessons learnt and
(c) provide mitigation measures, the follow up tasks – such as updates of security requirements/ measures/ procedures in an open manner for the benefit of EU, MS, business and citizens.

A strong geopolitical NIS related understanding and approach is required. This approach should consider a security life-cycle vision and a cooperation hub for EU cyber space. The neutral independent stakeholder should be able to work as a hub: with access to information while also having access to skillsets of other sectorial institutions. The neutral independent stakeholder should also be the proxy for worldwide collaboration as the context and impact of the cyber incidents are not contained by physical barriers anymore. In this case, collaboration with civil, military and LEA authorities is needed.

Lessons learned from other sectors. The above approaches do not differ from the approach taken in the Aviation industry where international cooperation complements national structures to secure the safety of the industry in a global context. Cybersecurity presents very similar challenges and similar solutions could be adopted in EU.

ENISA can play such a role, as a trusted third party, neutral independent stakeholder.

3. The evolution of ENISA mandate and current opportunities

3.1 Evolution of ENISA mandate

ENISA was set up by Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency[36] with an initial mandate valid for five years.

In 2008, Regulation (EU) no 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration[37] extended the validity of ENISA's up to March 2012.

By virtue of Regulation (EU) no 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency[38], the agency mandate was extended once more up to September 2013.

Finally, Regulation (EU) no 526/2013[39] of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 sets the latest mandate duration (expiring in June 2020).

While previous mandate renewals did not result in substantial changes in mandate, Regulation 526/2013 already streamlines and changes ENISA's duties in all domains. The table below compares Article 3 "Tasks" in Regulation 526/2013 with Article 3 "Tasks" in the repealed Regulation 460/2004; the evolution from original to current mandate sets the scene for the next mandate renewal.

Evolution of mandate

	Original 2004 mandate	Current 2013 mandate
Policy advice	• Collect […] information […] and provide the results of the analysis […] • Provide […] advice, and when called upon, […] assistance within its objectives	• Providing preparatory work, advice and analyses relating to […] policy and law • Assisting and advising on all matters relating to […] policy and law
	Specific reference to policy and law – clearer role for ENISA in the legislative process No reference to "when called upon" – possibility for ENISA to be more proactive	
Capability-building	• Enhance cooperation […] by organising […] consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts	(key words): support, knowledge, cooperation, raising level of capbility, exercises, collect/analyse/disseminate data, training

[36] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal L 077 , 13/03/2004 P. 0001 – 0011, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

[37] REGULATION (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC)No460/2004 establishing the European Network and Information Security Agency as regards its duration, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF.

[38] Regulation (EU) no 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, available at: https://www.enisa.europa.eu/media/news-items/extension-of-enisa2019s-mandate-published-1 .

[39] ENISA regulation (2013), Regulation (EU) No 526/2013 of 21 May 2013, in References section.

Evolution of mandate

	Original 2004 mandate	Current 2013 mandate
	• Facilitate cooperation […] in the development of common methodologies	
	Broad meaning of capability-building – more "hands on" support and assistnace	
Fostering cooperation and raising awareness	• Contribute to awareness raising and the availability of […] information […] by, inter alia, promoting exchanges of current best practices […] • Promote risk assessment activities […] solutions and studies	• Promoting best practices • Supporting […] in organising awareness raising […] and other outreach activities […]
	Broader scope of awareness activities – possibility for ENISA to support awareness-raising activities of other bodies, and to do other types of outreach	
R&D, and standardisation	• Assist […] dialogue with industry to address security-related problems • Track the development of standards for [security] products and services • Advise […] on research	• Facilitating the establishment and take-up of […] standards for risk management and […] security • Advising […] on research needs
	More than just "tracking" standards – possibility for ENISA to offer new services	
Cooperation with EU bodies and institutions	N/A	• Cooperate with Union institutions, bodies, offices and agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern [by]: ○ Exchanging know-how and best practices ○ Providing advice on relevant network and information security aspects in order to develop synergies
	Specific task related to cooperation with other bodies – clearer role for ENISA	
Third party outreach	• Contribute to […] efforts to cooperate with third countries and, where appropriate, with international organisations	• Contribute to […] efforts to cooperate with third countries and international organisations […] by: ○ […] observer and in the organisation of international exercises […] ○ Facilitating exchange of best practices ○ Providing […] expertise
	More specific tasks identified in the area of outreach – clearer role for ENISA in international cooperation processes	

3.2 Legal basis for ENISA activities

Articles 1-3 of Regulation (EU) no 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 establishes the scope, objectives and tasks of ENISA. The table below summaries the agency's main duties:

ENISA's current tasks as laid out in ENISA's founding regulation 526/2013	
Policy advice	• **Assisting and advising on** all matters relating to Union network and information security policy and law • Providing preparatory work, **advice and analyses** relating to the development and update of Union network and information security policy and law • **Analysing** publicly available network and information security **strategies** and promoting their publication
Capability-building	• **Supporting Member States**, at their request, in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, **and providing them with the necessary knowledge** • Promoting and facilitating voluntary **cooperation** among the Member States and between the Union institutions, bodies, offices and agencies and the Member States in their efforts to prevent, detect and respond to network and information security problems and incidents where these have an impact across borders • Assisting the Union institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, in particular by **supporting the operation of a Computer Emergency Response Team (CERT)** for them • Supporting the **raising of the level of capabilities** of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices • Supporting the organisation and running of Union network and information security **exercises**, and, at their request, advising Member States on national exercises • Assisting the Union institutions, bodies, offices and agencies and the Member States in their efforts to **collect, analyse and**, in line with Member States' security requirements, **disseminate** relevant network and information security **data**; and on the basis of information provided by the Union institutions, bodies, offices and agencies and the Member States in accordance with provisions of Union law and national provisions in compliance with Union law, **maintaining the awareness**, on the part of the Union institutions, bodies, offices and agencies as well as the Member States of the latest state of network and information security in the Union for their benefit • Supporting the development of a Union **early warning mechanism** that is complementary to Member States' mechanisms • Offering network and information security **training** for relevant public bodies, where appropriate in cooperation with stakeholders

Fostering cooperation and raising awareness	• Promoting **cooperation** between national and governmental CERTs or Computer Security Incident Response Teams (CSIRTs), including the CERT for the Union institutions, bodies, offices and agencies • Promoting the **development and sharing of best practices** with the aim of attaining an advanced level of network and information security • Facilitating **dialogue and efforts to develop and exchange best practices** • **Promoting best practices** in information sharing and awareness raising • Supporting the Union institutions, bodies, offices and agencies and, at their request, the Member States and their relevant bodies in organising **awareness raising**, including at the level of individual users, and other outreach activities to increase network and information security and its visibility by providing **best practices and guidelines**
R&D, and standardisation	• Facilitating the establishment and take-up of European and international **standards** for risk management and for the security of electronic products, networks and services • Advising the Union and the Member States on **research needs** in the area of network and information security with a view to enabling effective responses to current and emerging network and information security risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively
Cooperation with EU bodies and institutions	• **Exchanging know-how and best practices** • Providing advice on relevant network and information security aspects in order to develop **synergies**
Third party outreach	• Being engaged, where appropriate, as an observer and in the organisation of **international exercises**, and analysing and reporting on the outcome of such exercises • Facilitating exchange of **best practices** of relevant organisations • Providing the Union institutions with **expertise**

ENISA may also provide **advice** to union institutions, bodies, offices and agencies and Member State bodies **upon their request** and can **express independently** its own conclusions, guidance and **advice** on matters within the scope and objectives of its Regulation.

In addition, there are other instruments, with the same status as the founding regulation, that can be considered indirect extensions of the mandate as they give ENISA specific mandatory tasks. They include:

Tasks given to ENISA in other legislative instruments	
NIS Directive (2016)	• ENISA should **assist the Cooperation Group** in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council (7), […]. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident • In particular, ENISA should provide assistance [to the Cooperation Group] in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely **analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training** • ENISA should, in accordance with its mandate, support the **organisation and running of Union-wide exercises by providing its expertise and advice to the Cooperation Group and the CSIRTs network** • ENISA shall provide the **secretariat** and shall actively **support the cooperation among the CSIRTs** • **When adopting implementing acts** on the security requirements for digital service providers, **the Commission should take the utmost account of the opinion of ENISA** and should consult interested stakeholders • **ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered** in relation to already existing network and information security standards, including Member States' national standards regaring security requirements and incident notification

Tasks given to ENISA in other legislative instruments	
Payment services directive (2015)	• EBA shall promote **cooperation, including the sharing of information**, in the area of operational and security risks associated with payment services among the competent authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security • EBA shall **take into account standards and/or specifications** developed and published by the European Union Agency for Network and Information Security for sectors pursuing activities other than payment service provision
eIDAS Regulation (2013)	• ENISA is nominated as **recipient of notifications regarding breaches of security or loss of integrity** in 2 situations: ○ When multiple states are affected the notified SB (Supervisory body) should inform also ENISA • ENISA shall receive once a year a summary of notifications of breach of security and loss of integrity received from trust service providers (Summary report on breaches shall be submitted by 31/03 each year)
Directive on attacks against information systems (2013)	• The directive aims at **establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities**, including the police and other specialised law enforcement services of the Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, **and the European Network and Information Security Agency (ENISA)** • **Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA**, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level. For that purpose, the Commission should take into account the available analyses and reports produced by relevant actors and, in particular, Europol and ENISA
COM Regulation 611/2013 on the measures applicable to the notification of personal data breaches (2013)	• The Commission may, after having **consulted** the competent national authorities via the Article 29 Working Party, the European Network and Information Security Agency and the European Data Protection Supervisor, publish an indicative list of appropriate technological protection measures […] according to current practices
Other agencies' regulations, EU LISA regulation (2011)	• Mandatory for agencies, e.g. eu-LISA to **consult and follow up the recommendations** of the European Network and Information Security Agency regarding network security, where appropriate
Framework Directive 2002/21/EC as amended (2002) (Telecoms package Article 13a guidelines for NRAs)	• Where appropriate, the national regulatory authority concerned **shall inform** the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA) [**of a breach of security or loss of integrity** that has had a significant impact on the operation of networks or services]. Once a year, the **national regulatory authority concerned shall submit a summary report** to the Commission and **ENISA on the notifications received and the action taken** in accordance with this paragraph • The **Commission, taking the utmost account of the opinion of ENISA**, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements

3.3 ENISA strategy

The current mandate is refected in the ENISA strategy[40] and can be summarised as follows, with the 4 core objectives and one horizontal objective.

#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.

[40] ENISA strategy document, available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

3.4 Analysis of strengths and opportunities

3.4.1 Drivers for change

The change drivers identified are presented in four clusters: Strengths, Weaknesses, Opportunities and Threats (SWOT), as follows:

Internal	
Strengths	**Weaknesses**
• **Landscape view** – unique position to analyse how all MS are doing and communicate back • **Independence** – ENISA seen as an independent agency with no commercial or political bias • A **facilitator** – ENISA focuses on collaboration and community-building • **Needs-driven** – ENISA remains agile and able to respond to changing stakeholder needs • **Cybersecurity excellence** – at several levels, covering the complete security lifecycle	• **Growth** – pace of growth of budget and resources does not match pace of demand for ENISA involvement in new areas • **Influence** – ENISA has limited influence over industry • **Impact –** as with other EU institutions, ENISA needs a better methodology for tracking and understanding impact and addressing market needs
External	
Opportunities	**Threats**
• **SPOC –** opportunity for ENISA to be the primary/coordinating EU cybersecurity body • **Cybersecurity marketplace** – a role for ENISA in developing and supporting European cybersecurity products and services • **Public-private partnerships** – ENISA could be supporting and developing PPPs, e.g. leveraging the results of research and exploiting opportunities for EU products and services in the cybersecurity market • **Technology development** – opportunity for ENISA to be the reference organisation on cybersecurity implications from IoT, smart, mobile, AI • **Privacy and data protection** –ENISA could be given a role in assisting MS and EU in addressing the technical challenges of implementing data protection	• **Fragmentation** – the EU cybersecurity policy space has no coherent governance structure that includes all EU players in a complementary manner • **Strategic outlook –** difficulties in executing a long-term vision due to regulatory constraints and overlapping mandates (other agencies/bodies claiming to have expertise and ownership of cybersecurity)

3.4.2 Analysis of current tasks. Main findings

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

Rather the scope of the agency could be increased to ensure a more coherent approach to the entire cybersecurity life cycle: *Prevent – Detect – Respond*.

A number of current tasks need to be reinforced, namely *supporting the organisation and running of Union* ***network and information security exercises****, and, at their request, advising Member States on national exercises* in the capability-building domain and ***express independently its own conclusions****, guidance and advice on matters within the scope and objectives of its Regulation.*

The following have been put forward for consideration regarding ENISA's mandate, governance, role and responsibilities:

- 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 cybersecurity and give greater consideration to the economic and societal aspects of cybersecurity where ENISA could also play a role.
- Coordinating network information security and cybersecurity activities and response at EU level (ENISA as the EU *Single Point Of Contact* (SPOC) for cybersecurity incident response);
- Supporting the development of EU minimum standards on cybersecurity;
- Working with the EU Commission, having a better-defined role in research, including:
  - setting priorities for research in cybersecurity (policy and industry needs);
  - helping to transition cybersecurity research into the market place;
- Providing the EU Cybersecurity Information Hub;
- Establishing with industry a Cybersecurity Training Centre.
- Assessing awareness needs across EU-28, advise on "gaps", providing awareness material, coordinating awareness campaigns across the EU;
- Serving as the EU interface to bodies that are part of global cybersecurity response;
- In scoping ENISA's role and tasks, it would be important to define clearly the scope of different other actors in the EU cybersecurity space.
- A new governance structure along the lines being considered by other agencies could be suggested to improve the decision-making process.
- Analysing the economic and societal aspects and implications of cybersecurity (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.

ENISA's tasks list in Article 3 of ENISA regulation (2013) are not sufficiently strong in supporting NIS matters. The cybersecurity threat landscape now requires a more proactive, "hands on" approach. Regarding themes and role/responsibilities for ENISA, the following emerge as 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 cybersecurity.
- **Information** and **capability-building**: ENISA as the EU Cybersecurity Information Hub offering high quality cybersecurity analysis and training.
- **Cybersecurity lifecycle**: getting more involved in the complete cybersecurity lifecycle, including practical, "hands-on" support and an incident response (coordination) capacity.
- **Trends**: ENISA using its unique cybersecurity 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 cybersecurity 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 cybersecurity 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.

It is suggested that this approach allows the agency to maximise on its current capabilities. It is considered that the approach above demonstrates a pragmatic, incremental approach, which focuses on making the most of what ENISA already is doing and on a seamless evolution.

Several additional, more ambitious building blocks have been proposed in the next section. These are evidence of greater ambition for what ENISA could be doing in the long term and, depending on the course of future internal discussions and external negotiations, will also be pursued as future mandate building blocks.

3.4.3 Emerging strategic themes for ENISA's future mandate

On the basis of: (i) the mandate evolution and analysis in sections 3.1 and 3.2 and (ii) taking into account the SWOT analysis in section 3.4.1, a number of common strategic themes emerge. These are the main new building blocks of ENISA's future mandate. Items in the current mandate are not explicitly mentioned here.

A comprehensive mandate allowing for a coherent approach to EU cybersecurity

- 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

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

- 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 cybersecurity needs to be more explicit

ENISA as the EU Cybersecurity 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 (Cybersecurity Training Centre)

Involvement at all stages of the cybersecurity 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 cybersecurity debate
- Developing a response capacity to cybersecurity incidents, coupled with crisis management to complement at EU level the MS effort in this area (see next theme)

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

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

Using ENISA's enhanced cybersecurity 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 cybersecurity 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 cybersecurity on the basis of trends and needs

Maintaining and managing cybersecurity certifications

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

ENISA supporting standardisation and certification

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

ENISA supporting privacy and data protection in the cyberspace

- - Address the technical challenges of implementing privacy and data protection
- - Support the security of personal data

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 cybersecurity response
- Having specific powers to assist third countries with tasks falling within the ENISA mandate

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 cybersecurity 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 cybersecurity research and help with commercialisation
- In addition, there could be a role for ENISA in channelling/promoting and disseminating cybersecurity research results across Member States and industry

Contributing to the EU cybersecurity research agenda

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

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 cybersecurity

- Looking into the societal and economic dimension of cybersecurity 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 cybersecurity in the EU
- This would help ensure that cybersecurity 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

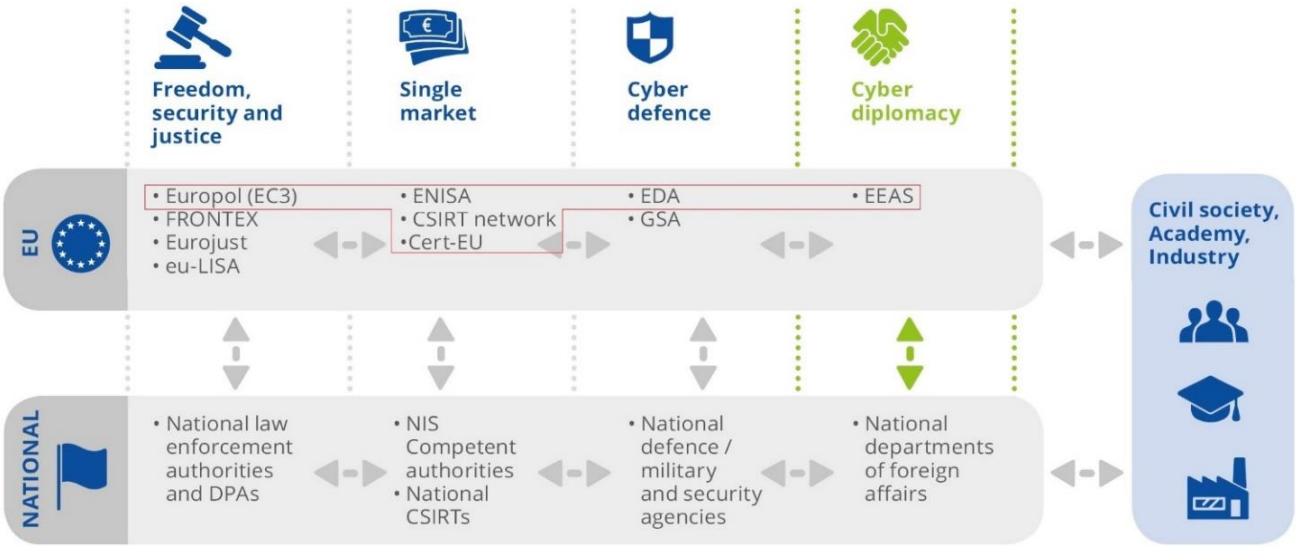
- Regarding governance arrangements:
  - retain Permanent Stakeholders' Group (PSG)
  - consider, in line with other EU agencies, an alternative governance structure for the agency, in order to improve efficiency of the decision-making process (NLO, PSG, Executive Board, Management Board (MB)).

4. Vision for the future

The associated picture illustrates the tasks that are proposed by ENISA for the new mandate.

The following sections provide description for each of the proposed new areas for the ENISA mandate, organised according to the ENISA strategic objectives[41].

Cyber coordination at EU level needs to be enhanced. There is a need to revise the current EU governance on cybersecurity, especially due to existing fragmentation of governance structure. There should be one entity that takes the lead on coordinating cybersecurity issues at a European level (see also section *'Cybersecurity coordination hub'* below). ENISA proposes that this be explicitly mentioned in its new mandate. In the following picture, compared with 2013 EU cybersecurity strategy, cyber diplomacy aspect was added.



[41] ENISA strategy available at: https://www.enisa.europa.eu/publications/corporate/enisa-strategy

4.1 Expertise: best practice & recommendations

Economics of cybersecurity (DSM)

The proposal is for ENISA to carry out studies of the **economics of cybersecurity** (i.e. the EU cybersecurity market and related economic issues) in order to provide quantitative data that could support decision making in this area. The overall goal would be to ensure that cybersecurity policy is aligned with EU industrial policy and that cybersecurity is used as an economic lever as opposed to a barrier.

Align cybersecurity research with policy & commercialisation

There are two ways in which ENISA can support to **align cybersecurity research with policy and commercialisation**. Firstly, to involve ENISA in high level panels that decide on research priorities for H2020 whenever cybersecurity is likely to be a key topic. Secondly, the Agency could work together with H2020 projects and its existing stakeholder networks to establish a framework to support the commercialisation of research results.

Coverage of geopolitical and societal developments

The existing work carried out by ENISA on the Threat Landscape should be broadened from the existing technical approach to **cover geopolitical, societal and economic developments**.

4.2 Policy: supporting policy development and implementation

Addressing cybersecurity policy fragmentation

The Commission should recognise the central role of ENISA in EU cybersecurity and use ENISA to minimise fragmentation and duplication of resources thereby **addressing cybersecurity policy fragmentation**.

ICT security certification

Current policy initiatives in this area are leading towards the creation of an EU framework for **ICT security certification**. As a neutral third party, ENISA would be an ideal candidate for supporting such a framework.

Involvement in all key policy initiatives

ENISA should be systematically alerted when new EU policy initiatives arise, which could have an impact on cybersecurity and privacy in the cyberspace ensuring **involvement in all key policy initiatives**. Such an alert should trigger a short analysis by ENISA identifying potential issues and suggesting whether or not the Agency should contribute. In addition, the Agency should be invited to contribute to policy development wherever it identifies a need to do so. The agency should provide strategic policy advice to the Commission, Parliament and the MS. This strategic level role can be added to the existing ones that are of tactical and support nature.

4.3 Capacity: hands on by ENISA experts

Cybersecurity full lifecycle

By combining preparation and response capabilities under a single EU body to provide a **cybersecurity full lifecycle** approach, the probability of incoherencies and misunderstandings would be greatly reduced. This could also reduce fragmentation at the EU level, eventually resulting in less independent organisations and enabling more powerful synergies and economies of scale. This would also increase the accountability of the Agency, as it would be implementing its own recommendations. In a system that splits these two aspects ('design' and 'implementation') there is scope for a misalignment at several different levels and the accountability model is not at all clear.

Reinforce role in securing CIIP

One of the main challenges of the NISD Cooperation Group (CG) is that the majority of the member states lack in depth knowledge on critical sector specific cybersecurity issues. At the same time, there is a lack of established and functioning at EU level bodies, which provide sector specific knowledge to the CG, which covers all different stakeholders and all different subsectors. To fill these gaps, the new mandate can **reinforce ENISA's role in securing CIIs** by taking advantage of the knowledge gained and the relationships established with the sector specific stakeholders by the Agency during all these years.

Supporting standards process

ENISA could play a stronger role in **supporting the cybersecurity standards process** by providing policy and technical guidance to Standards Development Organisations (SDO). In addition, the Agency could assist the Commission in defining future policy in this area by acting as an advisor to the standardisation roadmap.

4.4 Community: community building/coordination

Cyber crisis cooperation / technical support

An EU focal point for **EU cyber crisis cooperation** would support the exchange of information and foster situation awareness on cyber incidents and related crises. Member States and EU Institutions, in particular the CSIRTs Network, should form the foundation of this pool, which would need to be supported by a core capability at EU-Level. ENISA would be a legitimate candidate to host such core capability.

Cybersecurity coordination hub

There are many EU institutions and bodies involved in cybersecurity, each with its own specific mandate and responsibilities (examples include Commission DGs, CERT EU, EC3, EDA, EU LISA). This situation has the advantage of being able to offer cybersecurity services that are targeted to particular communities but could result in separate pools of incomplete information and incoherent methods across communities (including incompatible standards and methodologies). ENISA, acting as a **cybersecurity coordination hub**, shall support these different bodies by offering a number of 'cross-community support services' such as threat analysis, *cross-community trends analysis, trusted information exchange, advice on standards and certification practices, standard risk analysis techniques and taxonomies*. This will help to avoid fragmentation and duplication of resources.

Increased international cooperation

The proposal is that ENISA plays a **more active role in international cooperation**. Concretely, (a) ENISA shall be called upon to play a more proactive role in collaborating with international organisations having a role in cybersecurity (such as the OECD, ICANN, IETF, …) and (b) ENISA shall be tasked with supporting cyber dialogues led notably by the EEAS when cybersecurity is an issue.

Annex A: Terminology

While in this document, we do not aim to provide new definitions to cybersecurity and to cyber space, we work with the following understanding of the terminology:

- **Cyber space** is the time-dependent[42] set of connected tangible assets[43] (relying or depending on networks and internet like communication), infrastructures, systems and networks; Information; Users and all activities and interactions/communication including virtual ones.
- **Cybersecurity** covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of **cyber incidents.** Considering the different types of components of the cyber space, cybersecurity should cover the following attributes: **Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability** (for tangible systems, information and networks) **Robustness, Survivability, Resilience** (to support the dynamicity of the cyber space), **Accountability, Authenticity** and **Non-repudiation** (to support information security).
- **Cyber ethics.** Ethics are principles or standards of human conduct. Cyber ethics is a code of behaviour on the Internet[44]. Cyber ethics is the philosophic study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to do, and how this affects individuals and society[45].
- **Cyber hygiene** covers several practices[46] that should be implemented and carrying out regularly to protect users and businesses online.
- Any occurrence that has impact on any of the components of the cyber space or on the functioning of the cyber space, independent if it's natural or human made; malicious or non-malicious intent; deliberate, accidental or due to incompetence; due to development or due to operational interactions is called **cyber incident**. Also we call cyber incident any incident generated by any of cyber space components even if the damage/disruption, dysfunctionality is caused outside the cyber space.
- To support a 'grading' of cyber incidents, we define **cyber accidents** as any occurrence associated with cyber space causing *significant damage* to cyber space or any other asset (has performance impact, requires repairs, replacement) or causing *personal injury*.
- **Cyber investigation**. A process conducted for the purpose of cyber accident and incident prevention which includes the gathering and analysis of information, the drawing of conclusions, including the determination of causes and, when appropriate, the making of safety and security recommendations.
- **Cyber-attacks** cover all cyber incident triggered by malicious intent where damages, disruptions or dysfunctionalities are caused.
- **Cybercrime** refers to any crime/criminal activity facilitated by or using cyber space.

---

[42] Time dependency aspect presented in: Cyberspace: Definition and Implications, Rain Ottis, Peeter Lorents (2010), abstract, available at: https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html
[43] A survey identifying the components of cyberspace as presented in cyber space definitions is presented in: "Cyberspace – What is it?", Damir Rajnovic - July 26, 2012, available at: http://blogs.cisco.com/security/cyberspace-what-is-it
[44] https://www.microsoft.com/en-us/safety/online-privacy/cyberethics-practice.aspx
[45] https://en.wikipedia.org/wiki/Cyberethics
[46] https://www.enisa.europa.eu/publications/cyber-hygiene

- **Cyber sabotage** refers to any sabotage activity facilitated by or using cyber space.
- By cyber espionage we understand 2 types of espionage vectors: (a) **state espionage** (intelligence, when state actors are involved) or (b) **industrial espionage** (when commercial actors are involved).
- **Cyber-defense**[47] refers to a variety of defensive mechanisms that could be used to mitigate or respond to cyber-attacks.
- **Cyberwarfare** refers to any action by a state, group or criminal organisation facilitated by or using cyber space targeting another state.

[47] Kolini, Farzan and Janczewski, Lech, "Cyber Defense Capability Model: A Foundation Taxonomy" (2015), International Conference on Information Resources Management (CONF-IRM) 2015, Proceedings, Paper 32, available at: http://aisel.aisnet.org/confirm2015/32

Annex B: References

Year	Reference	Policy/legislation reference. Complete title and link
2016		
	The NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, available at: http://data.europa.eu/eli/dir/2016/1148/oj
	COM communication 0410/2016 on cPPP	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410
	COM decision C(2016)4400 on cPPP	COMMISSION DECISION of 5.7.2016 on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, Brussels, 5.7.2016, C(2016) 4400 final, available at (including link to the Annex): https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp
	COM Communication delivering on European Agenda on Security to fight against terrorism	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL, delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, Brussels, 20.4.2016, COM(2016) 230 final, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf
	Joint Communication on countering hybrid threats	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response, JOIN/2016/018 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018
	General Data Protection Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88, available at: http://data.europa.eu/eli/reg/2016/679/oj
	LEA DP Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, available at: http://data.europa.eu/eli/dir/2016/680/oj
	PNR Directive	Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, p. 132–149, available at: ELI: http://data.europa.eu/eli/dir/2016/681/oj
2015		
	Digital Single Market Strategy for Europe (DSM)	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe, COM/2015/0192 final, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
	Payment Services Directive	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 337, 23.12.2015, p. 35–127, available at: http://data.europa.eu/eli/dir/2015/2366/oj
	The European Agenda on Security	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE

		REGIONS, The European Agenda on Security, COM/2015/0185 final, available at:http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2015:0185:FIN
2014		
	eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114, available at: http://data.europa.eu/eli/reg/2014/910/oj
2013		
	Cybersecurity Strategy of the EU	JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyber space, JOIN(2013) 1 final, available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
	ENISA Regulation	Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, OJ L 165, 18.6.2013, p. 41–58, available at: http://data.europa.eu/eli/reg/2013/526/oj
	Directive on attacks against information systems	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14, available at: http://data.europa.eu/eli/dir/2013/40/oj
	Framework Financial Regulation	Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council, OJ L 328, 7.12.2013, p. 42–68, http://data.europa.eu/eli/reg_del/2013/1271/oj
	COM Regulation 611/2013 on the measures applicable to the notification of personal data breaches	Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, OJ L 173, 26.6.2013, p. 2–8, available at: http://data.europa.eu/eli/reg/2013/611/oj
2011		
	Council conclusions on CIIP	Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP), 2011, Adoption of Council conclusions, available at: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT
	EU LISA regulation	Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p. 1–17, Version consolidated, after amendments, available here: http://data.europa.eu/eli/reg/2011/1077/2015-07-20
2010		
	Internal Security Strategy for the European Union	An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf
	Digital Agenda	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245&from=EN
2002		
	Framework Directive 2002/21/EC as amended	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33–50, consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/21/2009-12-19
	ePrivacy Directive 2002/58/EC as amended	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 , 31/07/2002 P. 0037 – 0047, Consolidated version, after amendments, available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

enisa.europa.eu