Briefing
Implementation Appraisal

European Parliament

May 2017

The European Union Agency for Network and Information Security (ENISA)

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

This briefing is one in a series of 'Implementation Appraisals', produced by the European Parliament Research Service (EPRS), on the operation of existing EU legislation in practice. Each such briefing focuses on a specific EU law which is likely to be amended or reviewed, as foreseen in the European Commission's annual work programme. 'Implementation Appraisals' aim at providing a succinct overview of publicly available material on the implementation, application and effectiveness to date of an EU law, drawing on input from EU institutions and bodies, as well as external organisations. 'Implementation Appraisals' are provided by the EPRS' Ex-Post Evaluation Unit, to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

Summary

Information and communication technologies play an increasing role in modern-day life and in the creation of a digital society. To ensure further growth, significant investments in security are necessary.

Cybersecurity is a growing concern for citizens, influencing their digital activity. It is also a significant cost for the economy. In 2015, the estimated worldwide economic impact of cyber-attacks reached US$500 billion. The cybersecurity market in Europe was estimated at €20.1 billion.

The European Union Agency for Network and Information Security (ENISA) was established to support the EU and the Member States in enhancing and strengthening their ability to prevent, detect and respond to network and information security (NIS) problems and incidents. ENISA is part of the broader legal and policy environment, which includes the EU cybersecurity strategy and the recently adopted directive on security of networks and information systems across the EU.

EP committee responsible at time of adoption of the EU legislation: Industry, Research and Energy (ITRE)

Date of adoption of original legislation in plenary: 16 April 2013 (2010/0275(COD))

Entry into force of original legislation: 19 June 2013

Planned date for review of legislation: by September 2017, the Commission will 'review the mandate of ENISA to define its role in the changed cybersecurity ecosystem, including aligning it to the requirements of the NIS Directive, based on the recent public consultation and results of the ongoing evaluation', Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy. A Connected Digital Single Market for All (COM(2017) 228)

Timeline for new amending legislation: ENISA operates under Regulation (EU) No 526/2013 until June 2020. In view of the current cybersecurity environment, the Commission intends to present a new proposal by the end of 2017. The revision of Regulation (EU) No 526/2013 is presumed in Annex 2 of the Commission work programme 2017.

EPRS | European Parliamentary Research Service
Author: Anna Zygierewicz
Ex-Post Evaluation Unit

1. Background

Use of internet services by individuals in the EU

News (% individuals aged 16-74)	68 % (2015)
Shopping (% individuals aged 16-74)	65 % (2015)
Social networks (% individuals aged 16-74)	63 % (2015)
Banking (% individuals aged 16-74)	57 % (2015)
Music, videos and games (% individuals aged 16-74)	49 % (2014)
Video on demand (% households that have a TV)	41 % (2014)
Video calls (% individuals aged 16-74)	37 % (2015)

Source: *Use of Internet services by Citizens in the EU in 2016*, European Commission

According to Eurostat data on internet access and use statistics - households and individuals, 85 % of European households had access to the internet (fixed or mobile) from home in 2016. This share increased from 55 % in 2007. In 2016, 79 % of individuals were regular users (at least weekly) of the internet: 71 % of individuals in the EU-28 accessed the internet on a daily basis with a further 8 % using it at least once a week (but not daily). Eurostat data on internet advertising of businesses - statistics on usage of ads shows that in the EU in 2016, 77 % of businesses had a website, 45 % used social media and 25 % used internet advertising.

Cybersecurity and cybercrime

In 2015, 25 % of internet users in the EU experienced security related problems. According to a Eurobarometer report on cybersecurity,[1] the two most common cybercrime[2] situations experienced by internet users are discovering malicious software on their device (47 %), and receiving an email or phone call fraudulently asking for access to their computer, logins or personal details (31 %).

According to Eurostat,[3] security concerns deterred some internet users from certain activities: 19 % did not shop online, 18 % did not carry out banking activities and 13 % did not use the internet with a mobile device via wireless connection from places other than home.

Internet users express concern about cybersecurity (*selected answers*)

- 89 % avoid disclosing personal information online;
- 85 % agree that the risk of becoming a victim of cybercrime is increasing;
- 73 % are concerned that their online personal information is not kept secure by websites;
- 67 % are concerned that this information is not kept secure by public authorities;
- 68 % are concerned about experiencing identity theft;
- 66 % are concerned about discovering malicious software on their device;
- 63 % are concerned about being the victim of bank card or online banking fraud;
- 60 % are concerned about having their social media or email account hacked.

Source: *Cyber security*, Eurobarometer

The ENISA Threat Landscape Report 2016 points out that the top five threats are: 1) malware; 2) web based attacks; 3) web application attacks; 4) denial of services and 5) botnets; the definitions of which were provided by ENISA (see figure 1).

According to a 2017 PricewaterhouseCoopers (PwC) report,[4] the total number of security incidents detected by respondents rose to 42.8 million in 2015, an increase of 48 % over 2013; the equivalent of 117 339 attacks every day. The European cybersecurity market of products and services protecting organisations was worth US$22 billion in 2016 and is expected to grow at 8 % per annum to 2018, predominantly driven by increasing spend on services.

[1] 'Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein', EU Cybersecurity Strategy.

[2] 'Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)', EU Cybersecurity Strategy.

[3] 1 out of 4 internet users in the EU experienced security related problems in 2015, Eurostat.

[4] Cyber security: European emerging market leaders, PWC.

Actions taken by individuals in the EU due to cybersecurity concerns

During the past 3 years, 45 % of individuals in the EU installed or changed their antivirus software; 39 % became less likely to give personal information on websites; 36 % only used their own computer and 35 % only opened emails from people and addresses they know.

Source: Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer

According to the ENISA Annual Activity Report 2015, the worldwide cybersecurity market was estimated at US$75 billion in 2015 and forecast to grow to US$170 billion by 2020. The cybersecurity market size in Europe was estimated to grow from €20.1 billion to €24.4 billion in 2018. At the same time, the estimated worldwide economic impact of cyber-attacks has reached half a trillion US dollars. Global surveys cited in the report, find that 15 % of businesses faced a cyber-attack in the past year; estimated loss of the business revenue to cyber-attacks in three world regions amounted to: €81.3 billion for Asia and the Pacific; €62.3 billion for the EU and €61.3 billion for North America.

2. Current legislation

ENISA was established in 2004, based on Regulation (EC) No 460/2004. Regulation (EC) No 1007/2008 and the Regulation (EC) 580/2011 extended the ENISA mandate, with Regulation (EU) No 526/2013 concerning ENISA finally repealing Regulation (EC) No 460/2004 on 21 May 2013. The agency was established for a period of seven years beginning on 19 June 2013.

ENISA's priorities

- Expertise – anticipate and support Europe in facing emerging network and information security challenges;
- Policy – promote network and information security as an EU policy priority;
- Capacity – support Europe maintaining state-of-the-art network and information security capacities;
- Community – foster the emerging European network and information security community;
- Enabling – reinforce ENISA's impact.

Source: *ENISA Strategy 2016-2020*

ENISA is based in Heraklion, Crete, Greece, and has a branch office in Athens. Its budget is €11.2 million for 2017 (€11.1 million for 2016). As of 31 December 2015, ENISA had 69 staff members.

ENISA was established to contribute to a high level of network and information security (NIS) within the EU, to develop a culture of NIS in society and to raise awareness of NIS, thus contributing to the proper functioning of the internal market. As stated in the 2015 annual report, ENISA is a centre of expertise for cybersecurity in Europe. The agency 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.[5]

ENISA's main target group is public sector organisations, specifically EU Member States' governments and the EU institutions. The agency also serves the ICT industry (telecoms, internet service providers and IT companies); the business community, especially small businesses; network and information security specialists, such as computer emergency response teams; academia and the public.[6]

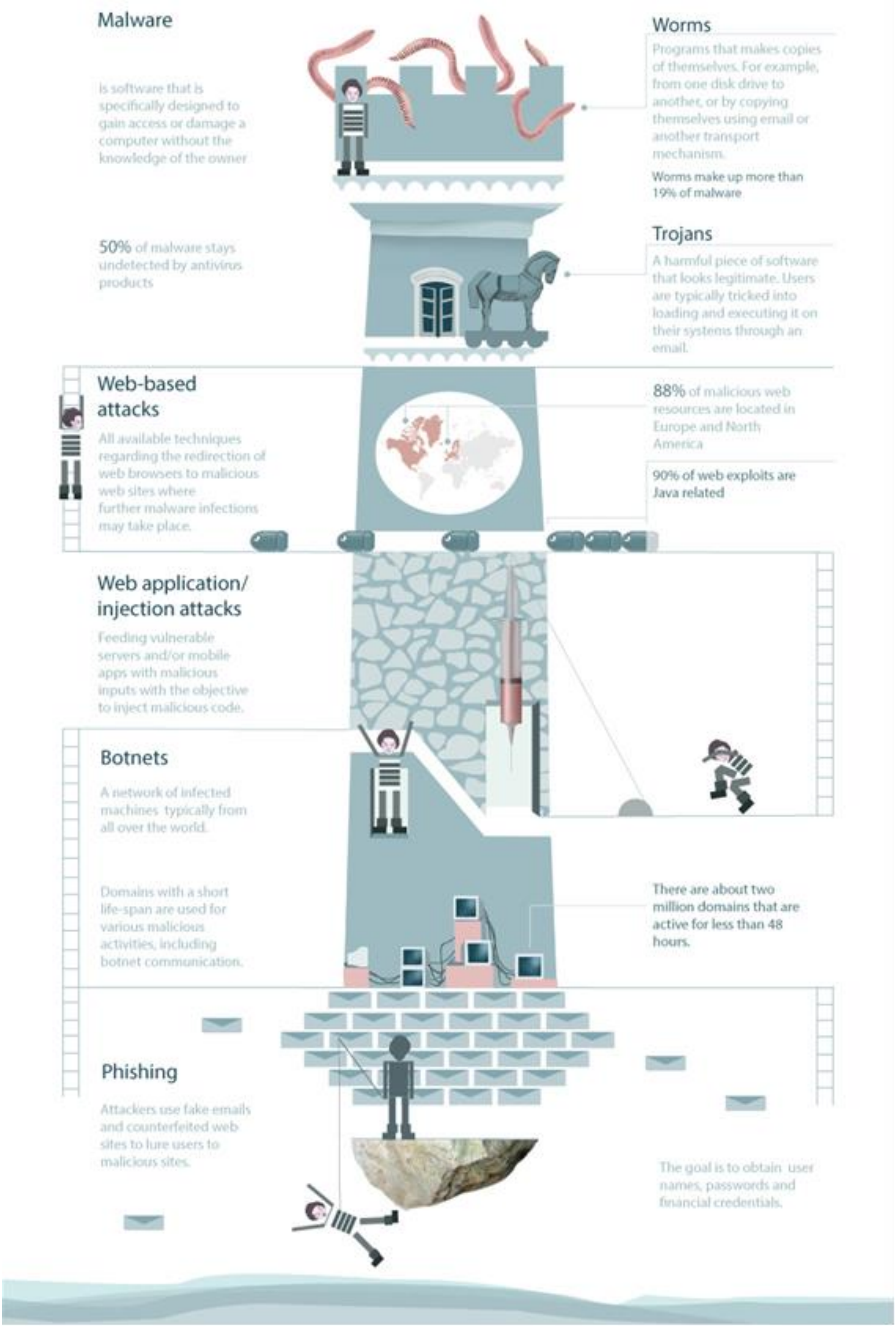
Among its activities, ENISA coordinates one of the biggest pan-European cybersecurity exercises, Cyber Europe,[7] every two years, which offers cybersecurity professionals the opportunity to analyse complex, innovative and realistic cybersecurity incidents. In 2016, the cyber exercises for participants ranged from forensic and malware analysis, mobile infection, malvertisement campaigns, open source intelligence, drones, etc. They are organised to prepare Europe for major cybersecurity crises at different levels: local, organisational, national, and European.

[5] The ENISA video 'Everything is connected' presents the role of the agency.

[6] Basic information on ENISA, European Commission.

[7] Cyber Europe 2016, Cyber Europe 2014, Cyber Europe 2012, Cyber Europe 2010, ENISA.

Figure 1. Cybersecurity. The top cyber threads



Malware

is software that is specifically designed to gain access or damage a computer without the knowledge of the owner

50% of malware stays undetected by antivirus products

Worms

Programs that makes copies of themselves. For example, from one disk drive to another, or by copying themselves using email or another transport mechanism.

Worms make up more than 19% of malware

Trojans

A harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems through an email.

Web-based attacks

All available techniques regarding the redirection of web browsers to malicious web sites where further malware infections may take place.

88% of malicious web resources are located in Europe and North America

90% of web exploits are Java related

Web application/ injection attacks

Feeding vulnerable servers and/or mobile apps with malicious inputs with the objective to inject malicious code.

Botnets

A network of infected machines typically from all over the world.

Domains with a short life-span are used for various malicious activities, including botnet communication.

There are about two million domains that are active for less than 48 hours.

Phishing

Attackers use fake emails and counterfeited web sites to lure users to malicious sites.

The goal is to obtain user names, passwords and financial credentials.

Source: European Parliament.

The ENISA Cyber Europe 2014 – After Action Report showed that the exercise allowed ENISA to learn lessons, propose recommendations and take concrete actions, which help to enhance cyber crisis preparedness in Europe. It also demonstrated that the common ability to mitigate large scale cybersecurity incidents in Europe has progressed since 2010 when the first Cyber Europe exercise was organised.[8]

ENISA vision statement 2020

By 2020 ENISA should:

- be 'the hub' for exchange of information on cybersecurity between the EU public sector and Member States;
- have developed its operational model (...) to provide seamless support to its stakeholders in all areas covered by the mandate;
- have an established presence in all key industry sectors and be a recognised name among security professionals;
- be able to demonstrate a positive contribution to EU economic growth through its initiatives.

Source: *ENISA Programming document 2017-2020*

ENISA prepares reports and recommendations. Recently the agency published a report on Cyber Security and Resilience of smart cars, which makes recommendations to smart car manufacturers, aftermarket vendors, insurance companies, researchers, industry groups and associations.

ENISA forms part of the broader legal and policy cybersecurity environment,[9] of which the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, adopted in 2013, forms a part. The strategy proposes specific actions to enhance the EU's overall performance, acknowledging that it is predominantly the task of Member States to deal with security challenges in cyberspace. The strategy is based on five strategic priorities: 1) to achieve cyber resilience; 2) to drastically reduce cybercrime; 3) to develop cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP); 4) to develop the industrial and technological resources for cybersecurity and 5) to establish a coherent international cyberspace policy for the European Union and promote core EU values.

The European Agenda for Security was adopted in 2015 to allow the EU to support Member States in ensuring security. The Agenda should stimulate better information exchange, increased operational cooperation and mutual trust, drawing on the full range of EU policies and tools. The Agenda pointed to 'terrorism, organised crime and cybercrime as interlinked areas with a strong cross-border dimension, where EU action can make a real difference'.

In 2016, Directive (EU) 2016/1148 on security of networks and information systems across the Union (NIS Directive) was approved, to 'lay down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market'.

In 2016, an EU cybersecurity public-private partnership[10] was launched, which should trigger €1.8 billion of investment by 2020. The EU will invest €450 million in this partnership within the Horizon 2020 framework programme for research and innovation. The partnership was established with the aim 'to foster cooperation at early stages of the research and innovation process and to build cybersecurity solutions for various sectors, such as energy, health, transport and finance'.

3. EU-level reports and evaluations

ENISA Annual Activity Report 2015

In its Annual Activity Report 2015,[11] ENISA stated that 2015 was a successful year, with the agency maintaining its track record of delivering according to plan and within its allocated budget. The agency strengthened relations with stakeholders and assisted them in making significant improvements to the

[8] The ENISA video 'Are you ready for the next cyber crisis?' presents the role of these exercises.

[9] A list of other policy references within which ENISA operates can be found in the ENISA's work programme.

[10] Commission Decision of 5 July 2016, C(2016) 4400

[11] Previously, ENISA published ENISA Annual Activity Report 2014 and ENISA Annual Report 2013.

state of cybersecurity throughout the EU. ENISA reported a total of 53 deliverables.[12] An annual Threat Landscape Report was also prepared in 2015.[13]

Highlights during 2015 included new best practices and recommendations in sectors such as eHealth, finance, and smart infrastructure and services. ENISA continued activities such as training Computer Security Incidents Response Teams (CSIRT), and preparations for Cyber Europe 2016. ENISA updated the Threat Landscape and published guidelines and best practice recommendations regarding privacy enhancing technologies[14]. The agency organised a number of events, such as the High Level Event, the first ENISA industry event, the Annual Privacy Forum and the EU Cyber Security Month campaign. It hosted workshops which gathered experts in the field to discuss cybersecurity topics.

Evaluation of ENISA's activities. Case study report – Work package 1.2 2015
Evaluation of ENISA's activities. Case study report – Work package 2.1 2015
Evaluation of ENISA's activities. Case study report – Work package 3.3 2015
prepared by Ramboll[15] at ENISA's request

An independent contractor, Ramboll, has conducted a three part evaluation of ENISA's work. The two first packages involved case studies of four deliverables, and a third covered two deliverables (all with a budget above €30 000:

a) Work package 1.2: D1: Stock Taking, Analysis and Recommendations on the protection of Critical Information Infrastructures (CIIs); D2: Methodology for the identification of Critical Communication Networks, Links, and Components; D4: Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector; D5: Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services.
b) Work package 2.1: D1: Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies (NCSS); D3: Maintain CERT good practices and training library; D4 - Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap; D5: Impact evaluations on the usefulness of the ENISA guidelines on capacity building.
c) Work package 3.3: D1: Readiness analysis for the adoption and evolution of privacy enhancing technologies; D4: State-of-the-art analysis of data protection in big data architectures.

The general opinion of the evaluators is positive; but recommendations for improvements were also presented. In package 1.2, it was confirmed during the assessment that the four deliverables contributed to providing advice and assistance to stakeholders of Critical Information Infrastructures (CIIs). In package 2.1, D1 and D3 in particular contributed to the dissemination of good practices regarding cybersecurity among public and private organisations. In package 3.3, both deliverables contributed to supporting the development and implementation of data protection and privacy regulation. As one of the recommendations, the evaluators advised improving the visibility of ENISA activities and publications.

Evaluation Roadmap, European Commission

The Commission's ENISA Evaluation Roadmap (starting in Q3/2016 and ending in Q2/2017) sets out the purpose and scope of the planned evaluation, i.e. to assess ENISA's performance in achieving its objectives, mandate and tasks, as laid down in Regulation No 526/2013 (retrospective analysis) and to provide the basis for a possible revision of the current mandate (forward looking analysis).

4. European Commission Public Consultation

The Commission undertook a public consultation on ENISA from 18 January 2017 to 12 April 2017. It aims to evaluate ENISA over the 2013-2016 period, with a view to a possible revision of the current mandate.

[12] A list of ENISA's 2015 work programme publications.
[13] The latest report, ENISA Threat Landscape Report 2016, was published in February 2017.
[14] The newest publication in the area is Privacy Enhancing Technologies: Evolution and State of the Art, ENISA 2017.
[15] Previously, Ramboll prepared Evaluation of ENISA's Activities Case Study Report – Cyber Europe 2014.

At the time of finalising this briefing, the Commission had not yet published the results of the public consultation.

5. European Parliament position/Members' questions

5.1. European Parliament resolutions (selected for 2014-2017)

European Parliament resolution of 16 February 2017 on the European Cloud Initiative

Parliament urged the Commission and the Member States' national authorities, in consultation with ENISA, to cooperate in establishing a safe and trustworthy digital infrastructure and to build up high levels of cybersecurity in compliance with the Network and Information Security Directive.

European Parliament resolution of 19 January 2016 on Towards a Digital Single Market Act

The resolution called for efforts to improve resilience against cyber-attacks, with an increased role for ENISA in particular. It also urged increased risk awareness and knowledge of basic security processes among users, particularly SMEs, to ensure that companies have basic levels of security, such as end-to-end encryption of data and communications and software updates, and to encourage the use of the security-by-design concept.

In its follow-up[16] to Parliament's resolution in relation to ENISA, the Commission responded that ENISA is closely involved in the preparatory work for the launch of the public-private partnership and will play a key role in the implementation of the NIS Directive.

European Parliament resolution of 21 May 2015 on financing the Common Security and Defence Policy

The resolution called for creation of a permanent link between EU bodies and agencies in the areas of internal security (Frontex, Europol, ENISA) and external security and defence (European Defence Agency, EEAS).

The Commission, in its response[17] to Parliament's resolution answered that further synergies have been developed between freedom, security and justice actors and CSDP (and beyond CSDP), mentioning e.g. EEAS, Frontex and Europol, but without mentioning ENISA explicitly.

5.2. Members' questions (selected for 2014-2017)

Written question by Viviane Reding (EPP, Luxembourg), 11 January 2017

In view of the cyber-attacks in the context of the US presidential election, experts' concerns and warnings of possible similar actions to be taken during the forthcoming elections in Europe, the Commission is asked about measures which it plans to take and the role of ENISA.

Answer by the European Commission

At the time of finalising this briefing, the Commission had not yet responded to this question.

Written question by Nicola Caputo (S&D, Italy), 25 August 2016

In relation to ENISA, the Member asked whether the Commission intends to submit an assessment of the agency with regard to the adequacy of its remit.

Answer by Günther Oettinger on behalf of the European Commission, 3 November 2016

The Commission is required to evaluate ENISA by 20 June 2018 and the possible modification or renewal of ENISA's mandate must be adopted by 19 June 2020. In view of the current cybersecurity landscape, the Commission aims to advance and finalise the ENISA evaluation by the end of 2017. Such evaluation will address the need to modify or extend ENISA's mandate.

Written question by Kostas Chrysogonos (GUE/NGL, Greece), 10 February 2016
Written question by Manolis Kefalogiannis (PPE, Greece), 09 February 2016

[16] SP(2016)220.

[17] SP(2015)470.

Both questions concerned the change of the seat of the agency.

Answer by Günther Oettinger on behalf of the European Commission to both questions, 26 April 2016

According to Regulation (EU) No 526/2013 the seat of ENISA is Heraklion (Crete) and the branch office is established in Athens. Any amendment would have to be made by agreement between the Representatives of the Member States, meeting at Head of State or Government level.

6. European Council

In relation to the ENISA 2015 report on cyber crisis cooperation and management

Referring to the ENISA 2015 report on cyber crisis cooperation and management, the EU Presidency invited delegations to consider ENISA's recommendations, *inter alia*, on creating an EU-level pool of cyber crisis experts and a cyber-crisis cooperation platform. The Presidency also asked for an opinion, *inter alia*, on the role which ENISA could play.

In relation to the ENISA Threat landscape 2015

Referring to the ENISA Threat Landscape 2015, the EU Presidency requested delegations consider the suggestions of the report, *inter alia*, on the need to disseminate cyber-threat knowledge to all players in cyberspace, including end users.

7. European Economic and Social Committee (EESC)

Strengthening Europe's Cyber Resilience system (TEN/608)

In its 2016 opinion, the EESC welcomed the Commission's intention to evaluate ENISA's mandate by the end of 2017 and hoped that a European authority for cybersecurity would be established, equivalent to the European Aviation Safety Agency. The EESC specified that the mandate of ENISA should be strengthened to more effectively increase cyber-attack threat awareness and response across the Union. It suggested expanding the role of ENISA to take more direct responsibility for cyber security education and awareness programmes, especially targeted at citizens and SMEs.

8. Other sources of reference

- Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU, European Parliamentary Research Service, STOA: study and presentation
- Cybersecurity and cyberdefence. EU Solidarity and Mutual Defence Clauses, Patryk Pawlak, European Parliamentary Research Service
- Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Policy Department C on Citizens' Rights and Constitutional Affairs, European Parliament
- Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Policy Department C on Citizens' Rights and Constitutional Affairs, European Parliament
- Cyber security: protecting crucial sectors from attacks, EuroparlTV, European Parliament
- EU cybersecurity initiatives: working towards a more secure online environment, European Commission
- Information Operations and Facebook, Facebook, Inc.

To contact the Ex-Post Evaluation Unit, please e-mail: EPRS-ExPostEvaluation@ep.europa.eu

Manuscript completed in May 2017. Brussels © European Union, 2017.

The opinions expressed in this document are the sole responsibility of the author(s) and do not represent an official position of the European Parliament. Reproduction and translation of this document for non-commercial purposes are authorized, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

www.europarl.europa.eu/thinktank (Internet) – www.epthinktank.eu (blog) – www.eprs.sso.ep.parl.union.eu (Intranet)