CYBERSECURITY – PART 1: ENISA REFORM

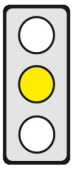
cep**PolicyBrief** No. 2018-06

Centrum für Europäische Politik

KEY ISSUES

Objective of the Regulation: Cybersecurity is to be increased and for this purpose the EU cybersecurity agency ENISA will be strengthened.

Affected parties: ENISA, Member States, companies



Pro: The improvement of cybersecurity is advisable and, in view of the cross-border dimension, must take place at EU level. Giving ENISA a permanent mandate and increasing its funding and staff is therefore appropriate.

Contra: (1) Assigning operational tasks to ENISA may mean that efforts are not made at national level ("freeriding").

(2) Clarification is required on whether Member States may reject investigations by ENISA, what actions ENISA can take and the extent to which it can use sensitive information.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2017) 477 of 4 October 2017 for a **Regulation** of the European Parliament and of the Council on **ENISA, the "EU Cybersecurity Agency**", and repealing Regulation (EU) <526/2013 and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

Brief Summary

- **Context and objectives**
  - According to the Commission, increasing digitisation and connectivity in many areas of society are leading to a rise in cybersecurity risks and attacks (Recitals 2 and 3).
  - The Commission therefore wants (Recital 5)
    - to improve cooperation between Member States and EU institutions, - agencies and -bodies,
    - increase the capabilities of Member States and businesses in combating cyber-attacks and
    - improve trust in the digital single market with more transparency about the level of security provided by information and communication-technology (ICT) products.
  - This will essentially be achieved by (Explanatory Memorandum p. 4 and 7, Recital 11)
    - reform of the Greece-based EU cybersecurity agency "ENISA" (this cep**PolicyBrief**) and
    - certification of the cybersecurity of information and communication technology (see cep**PolicyBrief**).
  - The proposed Regulation replaces the current ENISA Regulation [(EU) No. 526/2013].
  - ENISA was set up in 2004. As a centre of expertise for enhancing network and information security, it also supports the Member States. (Explanatory Memorandum p. 4, Art. 35)
  - In addition to minor organisational reforms, the ENISA reform covers
    - the establishment of a permanent mandate and an increase in its funding,
    - the transfer of additional functions and duties to ENISA.
- **Establishment of a permanent mandate, budget and staff of ENISA**
  - ENISA was given a fixed term mandate until 2020. It will now be made permanent. (Explanatory Memorandum p. 4, Art. 57 (4))
  - ENISA's budget is to go up from the current figure of € 11 million to € 23 million in 2022 (p. 102).
  - The staff of ENISA will increase from the existing 84 to 125 employees in 2022 (p. 98).
- **Main changes to the organisation of ENISA**
  - In future, ENISA will be able to set up offices in individual Member States where the Commission, Management Board and the affected Member State agree (Art. 12 (c), Art. 19, Art. 33).
  - In future, the Executive Board, which supports the Management Board, may pass provisional resolutions in cases of urgency, "in particular" on administrative management matters (Art. 12 (b), Art. 18).

Authors: Philipp Eckhardt and Dr. Anja Hoffmann | eckhardt@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-107 | www.cep.eu

- **Operational cooperation at EU level**
  - Until now, ENISA has "supported" the cooperation group and network of national computer emergency teams (CSIRTs) in the organisation of EU-wide cybersecurity exercises and advises Member States on national exercises at their request. In future, it will "organise" "annual" EU-wide exercises to prepare the cooperative response to "large-scale cross-border cybersecurity incidents" and support Member States in the organisation of these exercises at their request. (Art. 7 (6))
  - In future, ENISA will provide the secretariat of the CSIRTs network (Art. 7 (3) in conjunction with Art. 12 (2) NIS-Directive). It will support Member States within the network in improving their capabilities to "prevent, detect and respond to incidents"; it will analyse vulnerabilities, "artefacts" and incidents and, where requested, provide "technical assistance" in case of incidents which have a "significant or substantial impact" (Art. 7 (4)).
  - In future, ENISA will support or undertake ex-post investigations into reported incidents which have a "significant or substantial impact", if at least (Art. 7 (5))
    - two affected Member States request it or
    - two Member States are affected and the Commission in agreement with the affected Member States requests it.
  - In future, ENISA will prepare a regular "Technical Situation Report" on cybersecurity in the EU and support the development of a cooperative response to "large-scale cross-border incidents or crises related to cybersecurity" (Art. 7 (7) and (8)).

- **Development and implementation of EU policy and EU law**
  - As before, ENISA will contribute to the development and implementation of EU policy and law on cybersecurity by advising, supplying preparatory work and reviews (Art. 5). In future, it will also do this by way of
    - opinions, guidelines, the exchange of best practices on risk management and incident reporting under the Directive on network and information security [NIS Directive (EU) 2016/1148; see cep**PolicyBrief**] (Art. 5 (2)),
    - sector-specific strategies and law initiatives (Art. 5 (1)),
    - contributing its expertise to the work of the Cooperation Group which, in addition to ENISA, also consists of representatives of the Member States and the Commission (Art. 5 (3) in conjunction with Art. 11 NIS Directive),
    - providing advice and technical guidelines, as well as facilitating the exchange of best practices in the area of electronic identity and trust services, and to promote an "enhanced level of security of electronic communications" (Art. 5 (4), No. 1 and 2) and
    - providing an annual report on the state of implementation of EU law on breaches of security and loss of integrity reported by "operators of essential services" - inter alia energy suppliers -, by trust service providers and by telecommunications network operators and -service providers [Art. 5 (5) in conjunction with Article 10 (3) of the NIS-Directive see cep**PolicyBrief**, Article 19(3) of the eIDAS Regulation (EU) No. 910/2014, see cep**PolicyBrief**) and Article 40 of the European Electronic Communications Code (COM(2016) 590)].

- **Establishing capabilities and powers to combat cybersecurity incidents**
  - As before, ENISA supports EU agencies and Member States in the "prevention, detection and analysis" of cybersecurity incidents and in "capacity building" i.e. improving their capability to respond to cybersecurity incidents. Until now, Member States had to request this support. In future, ENISA will be able to act of its own accord with respect to Member States. (Explanatory Memorandum p. 8, Art. 6 (1) (a) and (b))
  - In future, ENISA will support Member States, at their request, in developing national Computer Security Incident Response Teams (CSIRTs) which monitor security incidents at national level, issue early warnings and react to them. In addition, it will support Member States, at their request, in the development of national strategies for the security of network and information systems and promote their EU-wide distribution. (Art. 6 (1) (c) and (d) in conjunction with Art. 7 (2) and Art. 9 (5) NIS Directive)
  - "Operators of essential services" are subject to special requirements for the security of their network and information systems; in particular, they must report security incidents to their competent authority or CSIRT (Art. 14 NIS Directive). Member States identify the "operators of essential services" in their territory (Art. 8 NIS-Directive). In future, ENISA will support Member States, in the context of the cooperation group, by exchanging best practices on the identification of "operators of essential services" (Art. 6 (1) (i) in conjunction with Art. 11 (3) (l) NIS Directive).
  - In future, ENISA will support the establishment of Information Sharing and -Analysis Centres (ISACs), particularly in sectors with operators of essential services (Art. 6 (2)).

Statement on Subsidiarity by the Commission

Due to the significant level of cross-border interdependence between network and information systems, individual players cannot handle threats to cybersecurity on their own. EU measures are therefore necessary.

Policy Context

The Directive on network and information security [(EU) 2016/1148, see cep**PolicyBrief**] was passed in 2016. In addition, the Commission submitted a Communication on strengthening Europe's cyber resilience [COM(2016) 410] in which it announced a review of the ENISA Regulation.

Legislative Procedure

4 October 2017	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content & Technology (leading)
Committees of the European Parliament:	Industry, Technology and Energy (leading), Rapporteur: Angelika Niebler (EVP Group, Germany)
Federal Ministries:	Federal Ministry for Home Affairs (leading)
Committees of the German Bundestag:	Home Affairs Committee (leading)
Decision-making mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Competence:	Art. 114 TFEU (Internal Market)
Type of legislative competence:	Shared competence (Art. 4 (2) TFEU)
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

According to information from the Commission, the economic impact of cyber-crime in the EU rose fivefold from 2013 to 2017 and could further quadruple by 2019 (Communication JOIN(2017) 450, p. 2). Cybersecurity incidents often affect more than one Member State. In addition, many EU countries do not have a security level which is adequate for dealing with the threat and thus they also jeopardise the other countries in the single market.

Considering this situation, the improvement of cybersecurity is appropriate and, in view of the cross-border dimension, must take place at EU level. Giving ENISA a permanent mandate and increasing its funding and staff is therefore appropriate. If ENISA acts as the central point for Member States to exchange information about cyber threats and -security incidents, coordinate activities and pass on best practice, this will reduce costs and boost synergies.

The additional step of **assigning operational tasks to ENISA, however, may mean that efforts** to strengthen cybersecurity **are not made at national level ("freeriding").** This danger exists in those Member States with only weak structures for defending themselves against cyber threats. This needs to be avoided. Apart from companies and citizens, Member States should also ensure cybersecure IT infrastructure because their proximity to the companies and citizens affected by security incidents often gives them a head start in acquiring knowledge which ENISA could only acquire by using up significant resources - it would ultimately have to set up a branch office in every Member State. Gains in efficiency are therefore unlikely to result from assigning operational tasks to ENISA.

ENISA should primarily take on a coordinating role. Consequently, some of ENISA's new tasks - such as the provision of "technical assistance", other operational support in the event of security incidents and their ex-post investigation - are not appropriate in the envisaged form. They will either result in unnecessary duplication of structures or there will be insufficient effort made at national level to introduce measures to strengthen cybersecurity. If these functions are nevertheless assigned to ENISA, Member States who wish to avail themselves of ENISA's help must also be required to pay for it.

ENISA's other operational tasks - such as joint cybersecurity exercises - offer real added value because the resulting exchange on effective strategies for reacting to security incidents may produce synergies and opportunities for learning which cannot arise to the same extent during exercises taking place purely at national level.

It is questionable whether the additional ENISA funds and staff - € 12 million, 41 employees - are sufficient for its new tasks. ENISA has already been given many additional non-operational tasks under the 2016 NIS-Directive, regarding e.g. the exchange of best practice in risk management, the notification of security incidents, setting up national Computer Security Incident Response Teams (CSIRTS) and the development of national strategies for the security of network and information systems. Experience with the NIS Directive should be gathered first before fixing ENISA's requirements for funds and staff to handle the cybersecurity tasks and before assigning operational tasks to ENISA.

Legal Assessment

Legislative Competency

In 2006, the European Court of Justice decided that the creation of ENISA and the transfer to ENISA of the duties provided for in the ENISA Regulation [(EG) No. 460/2004] was covered by the internal market competence (Art. 114 TFEU). The EU legislator has a broad scope for discretion regarding fields with complex technical features and, as a "measure for the approximation", can also transfer powers to a Union agency insofar as these tasks are closely linked to the objectives of a harmonisation package and are capable of supporting its transposition, application or uniform implementation (Case C-217/04, para. 44 et seq.; C-270/12, para. 103). This is also the case for an extension of ENISA's area of responsibility which aims to ensure the proper functioning of the internal market (Art. 1). ENISA's new tasks are closely related to the objectives of the NIS Directive and EU telecommunications law which also include the safeguarding of the integrity and availability of network and information systems - necessary for the functioning of the internal market. ENISA's work will and can (Art. 5 No. 2) facilitate the uniform transposition, application and implementation of this legislation. The Regulation is correctly based on Art. 114 TFEU.

Subsidiarity

Unproblematic. Member States cannot sufficiently ensure the collective cybersecurity of the EU by way of purely decentralised action. Coordination and support from ENISA is necessary to ensure the effective and uniform implementation of EU law. ENISA's operational powers to provide technical assistance on request in the event of serious security incidents and/or to support or carry out ex-post technical enquiries have greater value than national action primarily in cases where Member States – or their national CSIRTs – do not have sufficient capability to do this.

Proportionality with respect to Member States

It is unclear to what extent ENISA's new operational **powers to carry out** reviews and ex-post technical enquiries following security incidents (abbreviated as: **investigations**) **will be sufficient. Clarity is required as to** precisely **which actions ENISA can take** in this regard **and** whether it can also operate in Member States that refuse an investigation. Clarification is required on **whether Member States may reject investigations by ENISA** or can exempt certain sensitive areas and if so under what conditions – e.g. where in the Member States' view predominantly national (security) interests preclude it or only where the investigation extends to areas involving its – more narrowly defined – "national security", i.e. the existence or functioning of its state. Since national security falls under the exclusive responsibility of the Member States (Art. 4 (2), sentence 2 TEU), clarification, by way of a reservation of the right to refuse, is necessary at least for these cases.

In addition, Member States may refuse to issue information to ENISA where "essential security interests" prevent its disclosure (Art. 346 (1) (a) TFEU). **The extent to which ENISA can collect and use** security-related or other **sensitive information** – possibly against the will of a Member State – **and how it must protect this information, should also** therefore **be clarified.**

Compatibility with EU Law in other respects

ENISA's powers to carry out reviews and/or ex-post technical enquiries following security incidents could constitute an intervention in the affected companies' freedom to conduct a business (Art. 16 EU Charter of Fundamental Rights (CFR)) or to own property (Art. 17 CFR). Clear regulation is required on which actions are covered by these powers, particularly whether and under what conditions ENISA can undertake its own investigations – possibly against the will of the affected companies – and how confidential and commercially sensitive information can be appropriately protected in this regard. Without clear definition, these powers are disproportionate.

Impact on German Law

Since this is a Regulation which does not require transposition, primarily relating to the resources, budget and powers of ENISA, material changes to German law are not required.

Conclusion

The improvement of cybersecurity is advisable and, in view of the cross-border dimension, must take place at EU level. Giving ENISA a permanent mandate as EU cybersecurity agency and increasing its funding and staff is therefore appropriate. Assigning operational tasks to ENISA may mean that efforts are not made at national level ("freeloading"). The extent of ENISA's powers to carry out investigations following certain security incidents is unclear. Clarity is required as to which actions ENISA can take and whether Member States can refuse investigations by ENISA. The extent to which ENISA can collect and use sensitive information and how this information must be protected should also be clarified.