# *Agency Reform in the time of Cybersecurity Governance: ENISA*

by **ELENA PAURI**



## Abstract

L'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA) ha recentemente ricevuto dal Mediatore Europeo il premio per la Buona Amministrazione "Eccellenza nell'Innovazione", in virtù del suo progetto dedicato alla ridefinizione della cooperazione europea nel settore della sicurezza informatica.
Tuttavia, nonostante i notevoli risultati raggiunti in termini di qualità dell'output, in appena tredici anni di vigenza ENISA è stata soggetta a molteplici riforme che hanno modificato il suo regolamento istitutivo. Inoltre, ENISA è oggi soggetta ad un ulteriore processo di riforma. Alla luce dei risultati ottenuti dalla consultazione pubblica lanciata dalla Commissione Europea nel 2017, il presente articolo si occuperà dell'impatto che il sempre crescente rischio informatico ha sul cosiddetto "modello di agenzia europea". A tal fine sarà fornita, in primo luogo, una panoramica generale della normativa che regola ENISA. In secondo luogo, verranno analizzate le precedenti modifiche normative e le recenti proposte di riforma relative all'Agenzia, anche alla luce della dottrina tradizionale di settore. In seguito ci si interrogherà sulla capacità dell'Agenzia di rispettare i più elevati standard di diritto amministrativo rispetto alla "Dichiarazione congiunta e all'approccio comune" (*Joint Statement and Common Approach)* concordato nel luglio 2012 dal Gruppo di lavoro interistituzionale sulle agenzie decentralizzate dell'Unione europea. In conclusione verrà sostenuto che, come dimostrato dall'odierna minaccia nel settore della sicurezza informatica, vi è la necessità che le riforme delle agenzie europee assumano carattere meno frammentario e vadano oltre lo *status quo* attuale nella governance europea.

**1. Introduction.** In may 2017, a ransomware cyber-attack compromised hospitals' security in England and spread to more than 150 countries across the world. According to the European Cybercrime Centre (EC3), an observatory body set up in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus help protect European citizens, businesses and governments from

online crime, the financial cost of cybercrime for EU Member States (hereafter, MSs) is around €265 billion per year (EUROPOL 2017).

According to the European Commission, «[c]yber-security 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» (JOIN(2013)1 FINAL). The Commission has highlighted that cybersecurity is a high concern for many EU citizens in order to engage in e-commerce and for around a third of small to medium Enterprises to offer online services (COM/2010/245 F/2). According to a recent survey, at least 80% of European companies have experienced at least one cybersecurity incident over the 2014 (PWC.org 2017). If citizens and business owners lack confidence in security, it stands to reason that they may avoid participating in online activities, thereby inhibiting further development opportunities on cyberspace (ENISA 2014).

Notwithstanding existing threats, the benefits of cyber-reality are far superior to its disadvantages. Cyberspace offers an outstanding opportunity for social and economic growth, urging MSs and international organisations to tackle the issue of cybersecurity on the basis of mutual cooperation and information sharing. In fact, «national governments are best placed to organise the prevention and response to cyber incidents» (JOIN(2013)1 FINAL) and ENISA is called to be their expertise-based point of reference[1].

**2. The European Union Agency for Network and Information Security (ENISA) and EU cyber governance.** ENISA (hereafter, also “the Agency”) was set up in 2004 as a decentralised agency with the overall goal of ensuring a high level of network and information security (NIS) within the EU, thus contributing to the smooth functioning of the internal market (REGULATION (EC) NO 460/2004;

1 However, different policy approaches to coordination exist and they not always align. See, for instance, A. BOIN - M . BUSUIOC - M. GROENLEER, 2014.

MCKENNA 2004). ENISA has since supported European institutions, MSs and the business community in addressing, responding to and preventing NIS problems by developing and maintaining a high level of expertise in cybersecurity; supporting institutional cooperation and the implementation of EU policy; strengthening the MSs, EU institutions, agencies and bodies' capability and preparedness to prevent, detect and respond to NIS problems and incidents; identifying emerging trends and needs in view of evolving cybercrime and cybersecurity patterns. The Regulation also provides a definition of NIS as «the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and related services offered by or accessible via these networks and systems» (REGULATION (EC) NO 4 I60/2004).

The Agency was deemed to operate as a point of reference «establishing confidence by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in performing the tasks assigned to it» (*ibid*.). Thus, ENISA was provided with expertise-based advisory powers and the capacity to facilitate and promote cooperation among EU institutions, MSs as well as third countries (*ibid*.). The Agency has its seat in Heraklion and a secondary branch in Athens, Greece.

In line with the common EU agency structure and according to the latest amendments, the bodies of ENISA comprise a Management Board (composed by representatives from MSs and the Commission) which defines the general orientations for the operation of the Agency, an Executive Director appointed by the Management Board and responsible of the day-to-day administration of the Agency, and a Permanent Stakeholders Group (composed by experts from the ICT industry, e-communication providers, consumers, academia and representatives from MSs' regulatory authorities) chaired by the Director to perform advisory duties. ENISA's annual and multiannual working programmes as well as the final annual report are approved by the Management Board on

proposal by the Executive Director. The programme is then forwarded to the European Parliament, the Council, the Commission and the Member States and published. However, the Commission is the institution under which ENISA performs its mission. In fact, the Commission is involved in the appointment of the Agencies members, the proposal of the working programme and the drafting of the annual budget.

Since ENISA was first set up, it has been involved in raising awareness through publishing reports, organising expert workshops and developing public-private partnerships (CENCETTI 2014; MCKENNA 2013).

Thanks to its project on Redefining European cyber cooperation[2], ENISA recently received the EU Ombudsman Award for Good Administration for Excellence in Innovation.

**3. An evolving frame work: setting and early reforms.** Notwithstanding its incredible results in terms of output quality, in barely 13-years lifetime ENISA has gone through several reforms.

In 2008, an amendment to the Regulation establishing ENISA extended the mandate of the Agency for a period of 3 years. In fact, ENISA was first established for a period of 5 years so that its mandate was supposedly due to expire in 2009 (REGULATION (EC) NO 107/2008).

Following further debate, in 2009 the Council took the view that «[a]n enhanced and holistic European strategy for NIS, with clearly delineated roles of the European Commission, the Member States and ENISA, is of vital importance to tackle current and future challenges» (COUNCIL RESOLUTION 2009). However, notwithstanding the need to proceed with a thorough reform of the Agency mandate and powers, instead of amending Regulation (EC) No 460/2004, the duration of the Agency was once again extended until 13 September 2013 (REGULATION (EU) NO 580/2011).

2 A cyber-crisis simulation executed in real-time (over 48 hours) following two years of planning thanks to which training was provided to more than 1000 participants. See more at https://www.enisa.europa.eu/news/enisa-news/enisa-wins-award-for-excellence-in-innovation-transformation-at-eu-ombudsman-award-for-good-administration

With the Cybersecurity Strategy of the European Union (JOIN(2013)1 FINAL), the Commission gave new stimulus to the EU cybersecurity's policy. Even though the Strategy did not mean to amend ENISA's mandate, the Commission urged ENISA to perform particular tasks including the evaluation of the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs)[3] for the EU, the provision of technical guidelines and recommendations for the adoption of NIS good practices and the proposal of a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills of IT professionals (*ibid*.).

In 2013, a new Regulation (NO 526/2013) was provided to modernise and extend ENISA's mandate, also in view of the increasement of its links with Europol and industry stakeholders (COM(2013) 48 FINAL). Firstly, the Agency was given an increased budgetary allowance in order to support its contribute not only to the implementation of a high level of NIS but also to ensure better protection of privacy and personal data and the proper functioning of the internal market (REGULATION NO 526/2013). Secondly, the Agency was given new tasks, including the establishment and operation of a peer-review system to develop the CERTs capabilities (*ibid*.). Thirdly, the Agency was reformed in view of the need for it to be compliant with the principles of subsidiarity, independence, transparency and those laid down in the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies (*ibid*.). ENISA was also given new objectives, e.g. assisting the Union institutions, bodies, offices, agencies and MSs to meet the legal and regulatory requirements of NIS under existing and future legal acts of the Union (art 3.3) and tasks, e.g. disseminating data (art. 4(1)(b)(vi)) and facilitating the technical standardisation process (art. 4(1)(d)(i)). However, the

3 A Computer Security Incident Response Teams (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. A Computer Emergency Response Team (CERT) is developed in both private and public sectors in small teams of cyber-experts connected to the internet that can effectively and efficiently respond to information security incidents and cyber threats, often on a 24 hours a day-7days a week basis. See more about CERT-EU at https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html.

main change is perhaps to be acknowledged in the different approach the EU legislator adopts with regards to the best suited policy level to face modern cybersecurity threats. In fact, instead of maintaining its traditional understanding i.e. that MSs are best placed to engage in cybersecurity active policy, the EU now envisages to adopt new measures in accordance with the principles of subsidiarity and proportionality that «cannot be sufficiently achieved» by the Member States (*ibid.*).

The latest reform was long envisaged because of the evolving nature of the cybersecurity landscape. As mentioned in the 2013 Regulation, «[s]ince ENISA was set up, the challenges of NIS have changed with technology, market and socio-economic developments and have been the subject of further reflection and debate. In response to the changing challenges, the Union has updated its priorities for network and information security policy» (*ibid*.).

Hence, during the last two decades, the EU has repeatedly returned on its policies in the field of information security (NIS), data protection and security in electronic communication. Recently, multiple actions have been taken in order to foster the European Digital Single Market[4] and Agenda on Security in the field of cyber-related threats (COM(2015) 185 FINAL). For instance, the Commission is now setting out a new approach on interoperability of information systems (COM(2017) 261 FINAL).

Meanwhile, ENISA, Europol/EC3 and EDA have been playing an increasingly crucial role as EU-level agencies active from the perspective of NIS, law enforcement and defence respectively (CENCETTI, 2014).

However, notwithstanding its remarkable importance in view of the growing impact of cybersecurity on the market and the need to build transnational cyber-resilience, ENISA was once more given a fixed-term mandate, due to expire in the 2020 (REGULATION NO 526/2013).

4 The Digital Single Market strategy was adopted on the 6 May 2015 and includes 16 specific initiatives which have been delivered by the Commission. The strategy is now under review (see (COM)2015/0192 final). The Commission also recently launched a public-private partnership with representatives from the industry sector that is expected to trigger EUR 1.8 billion of investment by 2020 (see 2016 Cybersecurity Communication, *infra*).

**4. An evolving frame work: recent developments and the 2017 public consultation.** Moreover, ENISA is nowadays under a new revision process. In fact, ENISA's mandate and objectives were to be reconciled with the renovated cybersecurity landscape, which has evolved significantly in terms of threat, technological, market and policy developments. These developments include policy and regulatory measures, in particular those set out in the 'NIS Directive' and the 2016 cybersecurity Communication, which will result in "ENISA 2.0" (COM(2016) 410 final).

A public consultation took place between 18 January and 12 April 2017. It was conducted in the context of the evaluation and review of ENISA in accordance with Article 32 of Regulation (EU) No 526/2013. Respondents[5] from 19 different MSs mostly agree that, overall, the performance of ENISA during the 2013-2016 time span was positively assessed as contributing to NIS in the EU. A majority of respondents furthermore considered ENISA to be coherently achieving either to a great or some extent its individual objectives. Moreover, ENISA's output (services, guidelines, recommendations and reports) is appreciated for its EU-level body quality.

However, respondents made it clear that, due to the evolving cybersecurity landscape and the current EU policy response, some urgent needs and gaps, including cooperation across MSs, capacity to prevent, detect and resolve large scale cyber-attacks, information sharing between different stakeholders, and protection of critical infrastructure and improved education in cybersecurity, have to be addressed. In that respect, a limited number of available instruments at EU level seem adequate but ENISA, which is regarded as the most appropriate organisation to fulfil present expectations from the general public. In order to be

5 Out of 90 responses to the consultation, more than half of the respondents answered on behalf of an organisation (industry sector enterprises and representative associations), while others responded as professionals (in cybersecurity, telecommunications and government affairs) or in their personal capacity. Contributions from the public sector were comparatively low, though respondents representing national authorities were among the highest respondent group. The highest number of responses came from residents of Germany and Belgium (15 responses each), followed by respondents from Italy (7 responses), as presented in the figure below. See also https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-european-union-agency-network-and.

fully equipped for that mission, the Agency needs to be sufficiently mandated and resourced. The Commission is now carrying out an in-depth analysis of the replies to the public consultation which will be included into the overarching ex-post evaluation of ENISA, in accordance with the evaluation criteria set out in the EU Better Regulation Guidelines (COM(2015) 215 final) assessing the effectiveness, efficiency, coherence, relevance and EU added value of the Agency. The public consultation is also meant to contribute to a reflection on policy options for, once again, the revision of ENISA's mandate.

**5. Good administration and governance in the cyber area.** Given the above-mentioned multiplicity of interventions which ENISA's legal framework has been and still is undergoing, one is to argue whether the Agency was properly set up in the first place. In particular, it is not clear why ENISA's mandate has to be constantly renovated.

As Chamon (2016) correctly notices, notwithstanding its "regulatory agency" status, ENISA lacks one of the main features of the kind, i.e. the permanent nature of its mandate. It is common knowledge that EU agencies are bodies set up with legal personality by virtue of an EU secondary law tool in order to perform a technical, scientific or managerial mission in a specific sector at European level, with a certain degree of structural and financial independence even though subject to EU public law (BUSUIOC - GROENLEER - TRONDAL 2010; M. CHAMON 2016; CHITI 2002; CRAIG 2012; GERADIN - MUNOZ - PETIT 2005; HARLOW - RAWLINGS, 2014; MAJONE,1997; RITTBERGER - WONKA 2011). They usually are identified with decentralised bodies both in terms of institutional functions and geographical location. While a number of different classifications about agencies in the EU legal environment do exist[6] and the so-called "European agency model" is under construction[7], yet it is very important not to confuse EU regulatory agencies and executive agencies[8].

6 The EU institutional classification of EU law agencies can be found at https://europa.eu/european-union/about-eu /agencies_en. See M. CHAMON, cit., pp. 5-15.
7 The term is shaped on the famous article by G. MAJONE (cit).
8 However, the exact meaning of that divide is still subject to much controversy. Even though the

There is no apparent reason for ENISA being established as a non-permanent body. First, even in the early 2000s it was clear to the Commission that the "way forward", as it was called in its 2008 Communication (COM(2008)135 FINAL), was to be found in the sense of a growing need for agencification. Second, it was also evident that ENISA was supposed to be a regulatory agency, as it was and still is called «to be actively involved in the executive function by enacting instruments which help to regulate a specific sector» instead of being «responsible for purely managerial tasks» (COM(2002) 718 FINAL). Finally, the year before ENISA was set up, the framework Regulation for executive agencies (COUNCIL REGULATION (EC) NO 58/2003) clearly established that fixed-term duration is a typical feature of the latter only (CHAMON 2016).

One possible reason for the present and reiterated inconsistency in the system can be drawn out of the uncertain nature of ENISA's legal basis. In fact, the Agency was established having regard to article 114 TFEU (ex 95 TEC), i.e. the Treaty provision which allows the EU legislative power to adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in MSs which have as their object the establishment and functioning of the internal market. It is widely held in literature (OHLER 2006; VETTER 2005; MOK 2006; GUTMAN 2006; RANDAZZO 2007; all cited in CHAMON 2016) that the Agency was to be set up on a different basis or, at least, one including article 352 TFEU and the so-called "subsidiary powers doctrine"[9].

However, when the Court of Justice was called upon to annul ENISA's basic regulation on the basis of the inconsistency with the ratio of article 95 TEC, it departed from the opinion by AG J. Kokott and dismissed case by holding that

phenomenon of EU agencies draws on the previous US experience, similarities between the two should not be overestimated as the american federal governance presents a completely different legal framework (see also CJUE, Case 10-56, *Meroni*).

9 Article 352 TFEU allows the EU to adopt acts which are deemed as necessary to attain objectives laid down by the Treaties when the latter have not provided the powers of action necessary to attain them. However, there are authors who express views of a slightly different persuasion. For instance, CRAIG puts ENISA in the context of the "third wave" or "quasi-regulatory" agencies, i.e. the ones set up in the new millennium, which do not have legal base in art. 352 TFEU due to the turn in the Commission choice to establish new bodies on the basis of particular policy tasks to be performed.

«the establishment of a Community body such as the Agency was an appropriate means of preventing the emergence of disparities likely to create obstacles to the smooth functioning of the internal market in the area» (CJUE, C-217/04, *ENISA,* para. 62; BOUVERESSE 2006; HANSMANN 2006; FABIANO 2006; I. IGLEZAKIS, 2006).

The ruling is at least ambiguous in its reasoning. In fact, it is not evident how the creation of a new body should be regarded per se as a means towards harmonisation. On the contrary, it is quite clear that the non-permanent nature of ENISA played a crucial role in the Court's reasoning (CHAMON 2016). In fact, the EU judges argued that the Agency was given a mandate lasting for a period of five years only and that «the Community legislature considered that before making a decision as to the fate of the Agency it was appropriate to carry out an evaluation of the effectiveness of that Agency and the contribution which it makes to the implementation of the Framework Directive and specific directives» (Case C-217/04, cit., para. 65-67). It thus seems that the Court wanted to suggest that only an effective contribution to the harmonisation of national legislation would make sense of ENISA's very existence. In fact, that was the reason why the Agency had to be set up as a non-permanent body, notwithstanding its regulatory nature. Hence, ENISA is a body correctly established on the basis of the Treaty provision which empowers the EU legislature to harmonise national law only insofar as the Agency is a means to the tasks it was given, i.e. the removal of technical obstacles to the implementation of transnational cybersecurity in the internal market.

However, the mandate of the Agency should now be amended and kept on a fixed-term basis for a number of reasons.

First, it is the opinion of the author that the suitability of a legal basis for the establishment of a new body does not depend on material results performed by the body during its mandate. In fact, the appropriateness of a legal provision and the power it confers on EU institutions with reference to a certain objective are an *a priori* attitude of the norm and thus stay valid regardless of the actual results of the action based on the provision itself.

Second, the legitimacy of ENISA's standing is no longer questioned in

terms of output quality. The Agency has proven to be an example of administrative efficiency, praised by both the general public in the latest public consultation and the European Ombudsman's efficiency prize.

Third, in light of the increasing need for an expertise-based reference point in the field of NIS and cybersecurity, ENISA needs to be given a permanent status also for the sake of the continuity of its work. The issue at stake is even more sensitive if we consider that ENISA is called upon to play an ever greater role while lacking not only an adequate time-frame expectancy but also sufficient budgetary and HR resources[10].

In that respect, the present argument stands in contrast to the *2012 Joint Statement and Common Approach* by the Inter-Institutional Working Group on EU decentralised agencies[11]. In fact, the Statement recommends providing agencies' founding acts with either a sunset clause or a review clause, thus promoting the non-permanent body policy option.

However, it is important to underline that the Statement itself considers the process of closing down an agency to be a solution for bodies that are either underperforming or no longer relevant as a policy option. ENISA does not meet any of those preconditions. On the contrary, as demonstrated above, it is likely that there will be an increasing need for ENISA's service. In addition, a "periodic overall evaluation" envisaged in the Joint Statement (para. 60) would be sufficiently adequate in order to ensure ex-post control and to respond to performance concerns even without the provision of any mandatory sunset clause and, if necessary, to amend ENISA's basic Regulation or close it down accordingly.

Most recently, the European Commission announced the launch of a new proposal for a Regulation on the future of ENISA called the «Cybersecurity Act» (COM/2017/0477 final). As widely envisaged in the present paper and contrary to

10 The mentioned issues have been raised both in the past (see, for instance, EU Agencies Network 2014) and recently (see Euractiv.com) without any responsive echo among the general public.

11 The Inter-Institutional Working Group on EU decentralised agencies (IIWG) was launched by the the European Parliament, Council of the European Union and the European Commission in 2009 as a forum for inter-institutional dialogue.

any of the abovementioned critiques, the proposed article 57(4) explicitly provides that «[t]he Agency shall be established for an *indefinite* period of time starting from […]»[12]. It will now be up to the EU legislator whether to adopt such an act and so grant a more stable future for ENISA. In the meantime, the present landscape offers a great example of how technological innovation comes with spillover effects which are capable to drive administrative and legal reform.

**5. Conclusions.** A few remarks can now be drawn in conclusion. First, either an amendment to the Agency legal status or the introduction of a permanent mandate seem to be necessary in order for the ENISA's legal framework to comply with the principle of legal consistency among EU regulatory agencies. The European Commission already has taken advantage of the 2018 evaluation process in order to amend the Regulation accordingly. Second, the need for a stable point of reference in cybersecurity governance for the years to come urges the IIWG to review its position with regards to the so-called sunset clause in the drafting of agency frameworks for both the NIS and similar policy areas.

## References

A. BOIN - M. BUSUIOC - M. GROENLEER, *Building European Union capacity to manage transboundary crises: Network or lead-agency model?,* in *Regulation & Governance*, Vol . 8, 2014

A. BOUVERESSE, *Bases juridiques autorisant la création d'organismes dotés d'une personnalité juridique propre,* in Europe, nº 203, 2006

M. BOVENS, Analysing and Assessing Accountability: A Conceptual Framework, in *European Law Journal,* Vol. 13, 2007

M. BUSUIOC, *Accountability, Control and Independence: The Case of European Agencies,* in *European Law Journal,* 2009

M. BUSUIOC - M. GROENLEER - J. TRONDAL (eds), *The Agency Phenomenon in the European Union,* Manchester, Manchester University Press, 2010

C. CENCETTI, *Cybersecurity: Unione europea e Italia. Prospettive a confronto,* Roma, Ed. Nuova Cultura, 2014

M. CHAMON, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*, Oxford, OUP, 2016

E. CHITI, *Le agenzie europee: unità e decentramento nelle amministrazioni comunitarie*, Padova, Cedam, 2002

12 Enphasis on the word "indefinite" added.

G. CHRISTOU, *The EU's Approach to Cyber Security,* in *EUSC Working Papers,* A/W 2014
P. CRAIG, *EU Administrative Law*, Oxford, OUP, 2012
L. FABIANO, *Articolo 95 TCE e agenzie comunitarie: una nuova pronuncia della Corte di giustizia,* in Diritto pubblico comparato ed europeo, 2006
E. FAHEY*, The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security*, in *European Journal of Risk Regulation (EJRR),*Vol. 5, n. 1, 2014
D. GERADIN - R. MUNOZ - N. PETIT (eds), *Regulation through Agencies in the EU. A New Paradigm for European Governance,* Edward Elgar, Cheltenham, 2005
U. HANSMANN, *Schaffung der Europ. Agentur für Netz- und Informationssicherheit,* in Deutsches Verwaltungsblatt, 2006
C. HARLOW - R. RAWLINGS, *Process and Procedure in EU Administration*, Hart Publishing, Oxford, 2014
I. IGLEZAKIS, *case note*, in Elliniki Epitheorisi Evropaïkou Dikaiou, 2006
G. MAJONE, *The new European agencies: regulation by information*, in *Journal Of European Public Policy,* Vol. 4 , n. 2,1997
B. MCKENNA**,** *ENISA set to join Internet governance debate,* in *Computer Fraud & Security*, Vol. 2004, n. 10, 2004
B. MCKENNA**,** *ENISA surveys evolving threat landscape*, in *Computer Fraud & Security*, Vol. 2013, n. 1, 2013
L. LANGER - F. SKOPIK - P. SMITH - M. KAMMERSTETTER, *From old to new: Assessing cybersecurity risks for an evolving smart grid*, in *Computers & Security,* Vol. 62, Sept. 2016
B. RITTBERGER - A. WONKA, *Agency Governance in the European Union,* in *Journal of European Public Policy,* Vol 18, 2011
J. RUOHONEN - S. HYRYNSALMI - V. LEPPÄNEN, *An outlook on the institutional evolution of the European Union cyber security apparatus*, in *Government Information Quarterly*, Vol. 33, n. 4, October 2016
R. TAUWHARE, *Improving cybersecurity in the European Union: the network and information security Directive*, in *Journal of Internet Law,* Vol. 19, n. 12, 2016

**Jurisprudence**

Judgment of the Court of 13 June 1958, Case 10-56, *Meroni & Co., Industrie Metallurgiche, società in accomandita semplice v High Authority of the European Coal and Steel Community,* 1958 I-51
Judgment of the Court (Grand Chamber) of 2 May 2006, Case C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. [ENISA],* 2006 I-03771

**Legal acts and institutional documents (by date)**

Communication from the Commission, *The operating framework for the European Regulatory Agencies*, COM(2002) 718 final, Brussels, 11.12.2002
Council Regulation (EC) No 58/2003 of 19 December 2002, *Statute for executive agencies to be entrusted with certain tasks in the management of Community programmes*, OJ L 11, 16.1.2003
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,* L77/1, 13.03.2004
Regulation (EC) 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,* 18.10.2011 L 272/1
Council Resolution of 18 December 2009 *on a collaborative European approach to Network and Information Security*, OJ C 321, 29.12.2009

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 f/2)
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,* 24.6.2011 L 165/3
Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agenzie
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 Cyberspace*, Brussels, 7.2.2013 (JOIN(2013) 1 final)
European Commission, *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union,* Bruxelles, COM(2013) 48 final, 7.2.2013
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*, 18.6.2013 L 165/41
EU Agencies Network, *Position for annual exchange of views between EU agencies and European Parliament Committee on Budgets*, Brussels, 18 July 2014
ENISA, *An evaluation Framework for National Cyber Security Strategies*, November 2014
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on t*he European Agenda on Security*, Strasbourg, 28.4.2015 COM(2015) 185 final
European Commission, *Better Regulation Guidelines*, Staff Working Document, COM(2015) 215 final, Strasbourg, 19.5.2015
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) 410 final, Brussels, 5.7.2016
Communication from the Commission to the European Parliament, the European Council and the Council, *Seventh progress report towards an effective and genuine Security Union*, Strasbourg, 16.5.2017 COM(2017) 261 final and press release IP/17/1303, 16.5.2017
Proposal 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") COM/2017/0477 final