THE CONCEPT OF ACCOUNTABILITY IN THE CONTEXT OF THE EVOLVING ROLE OF ENISA IN DATA PROTECTION, EPRIVACY, AND CYBERSECURITY

W. Gregory Voss

This is an Accepted Manuscript of a book chapter published by Routledge in TECHNOLOGY AND THE LAW: ACCOUNTABILITY, GOVERNANCE AND EXPERTISE (edited by Alessandra Arcuri and Florin Coman-Kund) on 28 May 2021, available online: https://www.routledge.com/Technocracy-and-the-Law-Accountability-Governance-and-Expertise/Arcuri-Coman-Kund/p/book/9780367898571.

THE CONCEPT OF ACCOUNTABILITY IN THE CONTEXT OF THE EVOLVING ROLE OF ENISA IN DATA PROTECTION, EPRIVACY, AND CYBERSECURITY

W. Gregory Voss

1. INTRODUCTION

Agencies are seen as ideal for managing complex and technical issues, given their high specialisation and access to experts, and their being shielded from political influence. Their alleged distance from political influence allows them to take decisions based on technical considerations alone.[1] However, this same distance raises difficulties for accountability, in the sense of holding the agencies to account.[2] Furthermore, the independence of agencies' technical and/or scientific assessments has been described by the Commission as their '*raison d'être*'.[3] In the European Union, agencies have been used both for operational activities and for supporting decision-making.[4] Moreover, it may be more palatable for Member States to give power to EU agencies, rather than to the Commission, as Member States have representatives on agencies' boards.[5] Nonetheless, certain contributions to the literature now nuance views of EU agencies' independence in the face of different levels of supervision and control and requirements for accountability. Agencies' dependence on the Commission and the fact that they work as part of a network with Member State counterparts are mentioned in this regard.[6]

[1] Busuioc, E.M., 2013. European Agencies: Law and Practices of Accountability (Oxford University Press), at 25-26.
[2] *Id*. at 2.
[3] Chamon, M., 2010. 'EU Agencies: Does the Meroni Doctrine Make Sense', Maastricht Journal of European and Comparative Law, 17(3), 281-305, at 283-284 (citation omitted).
[4] Coman-Kund, F., 2012. 'Assessing the Role of EU Agencies in the Enlargement Process: The Case of the European Aviation Safety Agency', CYELP, 8, 335-367, at 335-336.
[5] Chamon, M., 2010, supra note 3, at 287.
[6] Vos, E., 2018. 'EU agencies on the move: challenges ahead', SIEPS 2018:1, at 34.

The number of EU agencies has grown steadily, through different waves, with a first wave in the 1970s, a second in the 1990s, and a third in the 2000s.[7] One EU expert agency, ENISA, is a member of the last wave, or 'third generation' of EU agencies, active in cybersecurity. ENISA was established by Regulation (EC) No 460/2004 (ENISA Regulation), with the original objectives of (1) enhancing the ability to prevent and to address network and information security problems, (2) providing advice to the European Commission (Commission) on network and information security issues, (3) using its expertise to stimulate cooperation between different actors, and (4) assisting the Commission in technical preparatory work on legislation in the field of network and information security.[8] This translated into rather soft powers being entrusted to ENISA, which helped this agency to survive a challenge to its very existence before the Court of Justice of the European Union (CJEU). [9]

ENISA has recently received additional responsibilities,[10] which make a discussion of its accountability all the more relevant for the period after such change. This is important, because logically the level of accountability-ensuring processes applied to agencies should vary with the degree of operational responsibility that an agency holds, as is recognised by Rocca and Eliantonio's analysis of agencies based on groupings related to soft law instruments[11].

This chapter demonstrates the increasing role of one EU agency—European Network and Information Security Agency (ENISA), prior to discussing the challenges that this raises with respect to accountability, and the part that the evolution of ENISA's governance structures may play in meeting such challenges. The *essential research question* is whether accountability is a concern for ENISA today, given the development of its powers and governance structures, and whether recent and potential future changes to the agency's role might necessitate a re-assessment in this respect. This study is conducted using the evolving legal-analytical framework of governance of decentralised agencies, as modified by the

[7] Chamon, M., 2010, supra note 3, at 283.
[8] Regulation (EC) No 460/2004, [2004] OJ L77/1, art. 2.
[9] Case C-217/04 *United Kingdom v Parliament and Council* EU:C:2006:279 l.
[10] This is as the result of the adoption of the EU Cybersecurity Act, which is discussed infra.
[11] Rocca, P. and Eliantonio, M., 2019. 'European Union Soft Law by Agencies: an Analysis of the Legitimacy of their Procedural Frameworks', SoLaR (Jean Monnet Network on the study of EU soft law by national administrations and courts) Publication, at 15-30.

Common Approach on EU Agencies,[12] and then handling ENISA as a legal-empirical case-study with the specificities related to its role in EU legislation and 'soft law'.

This chapter begins by providing an overview of theoretical perspectives regarding the accountability of EU agencies relevant for assessing ENISA's accountability (Section 2), followed by a brief description of ENISA as an expert body (Section 3). Next, the role of ENISA in connection with EU legislation that has developed over recent years in the areas of data protection, eprivacy and cybersecurity, is detailed (Section 4). An early challenge to ENISA's legal basis is then discussed (Section 5), prior to detailing the evolution of ENISA's mandate, as evidence of its establishment as an agency with growing importance (Section 5), and the evolution of ENISA's governance structures, as one solution to accountability challenges (Section 7). Finally, additional comments on accountability in connection with ENISA are made (Section 8), prior to concluding (Section 9).

2. Theoretical perspectives on EU agencies' accountability

The underlying concept of accountability is broad, and the quest for it has become pervasive. It may be viewed on different levels and has been seen to convey 'an image of transparency and trustworthiness'.[13] According to Curtin, accountability may be divided up into two categories: that concerned with making decision-making more democratic (political or democratic accountability), and that concerned with controlling delegated powers (administrative or bureaucratic accountability).[14] In a more granular analysis, Vos identifies five types of accountability: managerial (here the management board is important), political (involving the Parliament and the Council), administrative (where the Ombudsman is important), financial (involving the Commission's financial controller, the Court of Auditors, the Council and the Parliament) and judicial (involving the CJEU). She refers to this accountability as ex-post control and describes it as carrying out a 'retrospective process of information, discussion and evaluation of agencies' actions.'[15]

[12] Joint Statement of the European Parliament, the Council of the EU and the European Commission on decentralised agencies of 19 July 2012 (Common Approach on EU agencies) <http://europa.eu/about-eu/agencies/overhaul/index_en.htm>.
[13] Curtin, D., 2009. Executive Power of the European Union. Law, Practices, and the Living Constitution (Oxford University Press), at 246.
[14] *Id*. at 247.
[15] Vos, E., 2018, supra note 6, at 42.

Busuioc is quick to distinguish between control and accountability, cautioning that although the two terms have been used interchangeably, the former term is broader than the latter, and may include both 'ex ante and ex-post mechanisms of directing behaviour',[16] but do not involve actors having to 'explain and justify their conduct to forums'.[17] When Busuioc refers to accountability, she refers to principals delegating power or authority to agents, instead. Furthermore, she speaks of three kinds of control: ex ante control, ongoing control and ex post control, the latter of which she sees as synonymous with accountability,[18] similarly to Vos. In the case of ENISA, one could say that ex post control has been paramount, and that any need for ongoing control, as defined by Busuioc,[19] has in a way been obviated more or less by ex ante control, fashioned by constant repealing and replacing of the agency's foundational regulation, culminating in the Cybersecurity Act. Moreover, Busuioc highlights the importance of distinguishing between control and accountability in the case of European agencies, where independence necessitates excluding the kind of direct control that could be exercised as ongoing control.[20]

In Craig's discussion of agency accountability, control and accountability are divided into three sorts: legal, political, and financial.[21] His use of the term 'legal accountability' includes judicial review,[22] which is separated out by Vos as 'judicial accountability', and of perhaps less interest to our discussion of ENISA today. This is because, although the CJEU has competence to 'review the legality of acts of bodies, offices or agencies of the Union intended to produce legal effects vis-à-vis third parties' under Article 263 of the Treaty on the Functioning of the European Union (TFEU),[23] ENISA does not make formal decisions having such effect.[24] Concerns of democratic control and the rule of law arise in the case of authorities that have direct law enforcement power;[25] but ENISA does not exercise such

[16] Busuioc, E.M., 2013, supra note 1, at 48 (citation omitted).
[17] *Id*. at 49.
[18] *Id*. at 52.
[19] Busuioc refers to 'direct interference of the principal post-delegation' in the context of ongoing control. *Id*. at 51. This does not seem to apply to the ENISA case.
[20] *Id*. at 52.
[21] Craig, P., 2018. EU Administrative Law (Oxford University Press, 3rd edition), at 174-189.
[22] *Id*. at 176-177.
[23] Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, [2012] OJ C326/47 [herein TFEU], art. 263.
[24] This having been said, Craig cautions that if the Commission makes such formal decisions, in reality in most instances it follows the recommendations of the agency, and that then the agency should be subject to review. Craig, P., 2018, supra note 21, at 176.
[25] Scholten, M., Luchtman, M. & Schmidt, E., 2017, 'The proliferation of EU enforcement authorities: a new development in law enforcement' in the EU in Law Enforcement by EU Authorities: Implications for Political and Judicial Accountability 1-27, at 1 (Scholten, M. & Luchtman, M., eds., Edward Elgar Publishing).

powers.[26] Thus, when Scholten and Luchtman focus on judicial and political accountability in the context of what they define as EU enforcement authorities (EEAs),[27] such analysis does not have the same application to agencies such as ENISA. Most of our discussion on governance here (especially, Section 7) will relate to what Curtin has referred to as administrative accountability, and our earlier discussion of legislation (Section 4) will deal more with concepts of political accountability, as will our additional comments in Section 8. That having been said, we will also touch upon managerial and financial accountability, as those terms are used by Vos, and potential changes set out in our concluding remarks (Section 9) could one day make judicial accountability germane, as well.

However, depending on the facts relating to any particular agency, mechanisms implemented to ensure accountability (whether administrative or political) may be too extensive or inadequate, within a range going from 'high intensity', on the one hand, to 'undersight' and 'passive principals', on the other hand.[28] Busuioc states that, 'Agencies possess a variety of powers. Some have only information providing powers, whereas others can wield much more far-reaching powers. It is the latter that are more relevant from an accountability perspective. Substantively, accountability issues are most pertinent for the more powerful agencies'.[29] It may be argued, then, that the evaluation of the level of accountability obligations may change over time as the mandate of an agency evolves. By this it is meant that such obligations may be seen as either excessive (evidencing 'accountability overload') or inadequate, depending on the then-current mission of the agency and its powers, among other factors. Accountability becomes more important as an agency gains power, such as obtaining rulemaking authority or the ability to take actions intended to produce legal effects with respect to third parties. Furthermore, according to Vos, practices of Member States using EU agencies—for example, the European Union Aviation Safety Agency (EASA)—to represent them internationally or otherwise 'borrowing' the EU agencies, adds 'to the complexity of their accountability'.[30]

Administrative accountability could become an issue if an agency's action lacks transparency, or if it does not properly administer its budget. Furthermore, if an agency gains more actual influence, for example becomes more influential in policy-making, should it be not be subject

[26] *Id*. at 25. This continues to be true following the EU Cybersecurity Act.
[27] *Id*. at 9.
[28] Busuioc, E.M. & Lodge, M., 2016. 'Reputation and Accountability Relationships: Managing Accountability Expectations through Reputation', Public Administration Review, 77(1), 91-100, at 91.
[29] Busuioc, E.M., 2013, supra note 1, at 42-43.
[30] Vos, E., 2018, supra note 6, at 20.

to greater political and judicial control? For example, if an agency issues soft-law instruments such as recommendations, and these are taken up as the basis for assessment with data protection law compliance and result in sanction of a data controller, would this not become an issue of political and judicial control? These issues lead us to look to governance structures and discuss accountability in the context of ENISA further.

3. ENISA as an expert agency

ENISA's objectives led to tasks that included risk analysis, advice-giving, assistance within the scope of its objectives, enhancing and facilitating cooperation between various stakeholders and also between the Commission and Member States, organising consultations, contributing to conscience-raising, tracking the development of standards, contributing to European Community efforts to cooperate internationally 'to promote a common global approach to network and information security issues', amongst others.[31] Indeed, one of the expectations for EU agencies generally is 'to ensure better involvement for stakeholders in Union's policy fields and to develop networks, thereby stimulating the pooling of relevant information and best practices.[32] ENISA seems to fulfil this expectation. As one example, in the European Union, with respect to cybersecurity, ENISA tracked the work of Standard Development Organizations (SDOs) on standards on Network and Information Security (NIS), indicating areas where 'further work is necessary' and facilitating cooperation between SDOs and relevant EU organisations and industry. It encouraged public-private cooperation in these matters.[33] Although ENISA itself is not an SDO, it participated in identifying standards. According to one scholar:

> the Commission and international bodies organized in various forms establishing initially non-binding standards, which by reference or explicit incorporation by EU agencies into Union policies can become binding.[34]

[31] *Id*., art. 3.
[32] Coman-Kund, F., 2018. *European Union Agencies as Global Actors: A Legal Study of the European Aviation Safety Agency, Frontex and Europol* (Routledge), at 24-25.
[33] Purser, S., 2014. 'Standards for Cyber Security' in *Best Practices in Computer Network Defense: Incident Detection and Response* (M.E. Hathaway, ed., IOS Press), at 104, https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security.
[34] Hofmann, H.C.H., 2016. 'A European Regulatory Union – The Role of Agencies and Standards' in Research Handbook on the EU's Internal Market (Koutrakos, P. and Snell, J., eds.) (Elgar Publishing, Cheltenham, 2016), https://ssrn.com/abstract=2745252, at 471.

Thus, from the outset ENISA's role may have been greater than assumed at first glance. However, it still fell within the category of agencies supporting decision-making—Craig refers to it as an information and coordination agency,[35] a category perhaps less relevant from the standpoint of accountability than other categories of agencies—regulatory, decision-making, and quasi-regulatory.[36] Yet, its domain of expertise has become of crucial importance today with various incidents of 'hacking' and the exposure of vulnerabilities of key computer networks and systems,[37] and we may consider that its area of expertise is of interest to each of the three former pillars, as cybersecurity involves commercial interests, security and defence, involving 'dichotomies such as 'internal/external, public/private, civilian/military'.[38]

Core operations department (COD) units through which ENISA works are Secure Infrastructure & Services Unit, Data Security & Standardisation Unit and Operational Security Unit.[39] COD also includes the policy office, the public affairs team and support staff for the Advisory Group and the national liaison officers network[40], and operational staff has constituted approximately two-thirds of total staff, with the remainder being administrative staff and 'neutral'[41]. Stakeholders relations and administration department units of ENISA include Corporate Services and Stakeholders Unit, Finance and Procurement Unit, and Human Resources Unit.[42] At 31 December 2018, by contract type, 57% of ENISA employees were temporary agents; 39% were contractual agents; and 4% were seconded national experts.[43] More than 37% of in-house statutory staff was of Greek nationality; more than 11% dual-nationals; 7% each for Romanian and Italian nationalities; nearly 6% each for Belgian and Portuguese nationalities; and less for the other Member State nationalities.[44] ENISA

[35] Craig, P., 2018, supra note 21, at 166.
[36] *Id*. at 163-165.
[37] Craig notes that ENISA was established 'because of the increased importance of communication networks and information systems to modern economic and social development. The security of such networks is important, more especially given that this can be jeopardized by accident, attack, and mistake.' *Id*. at 166.
[38] Carrapico, H. & Barrinha, A., 2017. 'The EU as a Coherent (Cyber)Security Actor?', JCMS, 55(6), 1254-1272, at 1255.
[39] ENISA, Annual Activity Report 2018, Annex 1 Human Resources, A.1.1 Organisational Chart, at 54, https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2018.
[40] ENISA, ENISA Programming Document 2019-2021: Including multiannual planning, work programme 2019 and multiannual staff planning, Amendments, June 2019, at 51, https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021-with-amendments.
[41] *Id*., Annex 1 Human Resources, A.1.4 Information on Benchmarking Exercise, at 56. Information on the evolution of headcount may be found in Table 1'ENISA Budget and Temporary Agent Posts'.

[42] *Id*., Annex 1 Human Resources, A.1.1 Organisational Chart, at 54.
[43] *Id*., Annex 1 Human Resources, A.1. 5 Human Resources Statistics, at 57.
[44] *Id*.

provides a breakdown of its staff by activity: in 2018, approximately 15% of its actual staff (actual full time equivalents) was involved in expertise: 'anticipate and support Europe in facing emerging network and information security challenges'; close to 29% in policy: 'promote network and information security as an EU policy priority'; nearly 12% in capacity: 'support Europe in maintaining state-of-the-art network and information security capacities'; about 13% in community: 'foster the emerging European network and information security community'; and the remaining more than 31% in enabling: 'reinforce ENISA's impact'.[45] While each of these activities calls for knowledge in ENISA's domain of competence, it is perhaps the first category—expertise—which seems the most technical, involving 'collating, analysing and making available information and expertise on key NIS issues potentially impacting the EU taking into account the evolutions of the digital environment'[46].

In order to recruit expertise, there is a 'careers' page on ENISA's website listing open vacancies for seconded national experts (SNEs), trainees, temporary agents, temporary agents-inter-agency, contract agents, and undergraduate student programme.[47] Applicants for positions must be EU Member State nationals, and unsolicited applications are not reviewed. A Selection Board vets applications and draws up the candidates' reserve list, for the Executive Director's decision 'in line with post and budget availability, as well as considering a geographical diversity and a gender balance'[48]. A Management Board decision lays down requirements for the recruitment of SNEs through a transparent procedure, with applications handled through Member State permanent representatives[49]. Furthermore, calls for tender/calls for expression of interest of external support and reserve NIS experts for assistance are used.[50]

4. EU Legislation, 'Soft Law', and the Role of ENISA

Cybersecurity is an important issue for creating trust in the digital environment and a strategic issue for the European Union. This has been highlighted in the Commission's digital single

[45] *Id*., Annex 1 Human Resources, A.1.6 Human Resources by Activity, at 58.
[46] *Id*., Part I Achievements in the Implementation of the 2018 Work Programme, at 17.
[47] ENISA, Careers, https://www.enisa.europa.eu/recruitment/vacancies (last visited on 8 February 2020).
[48] ENISA, Frequently Asked Questions (FAQ) for candidates applying to selection procedures, Version No. 5, July 2019, https://www.enisa.europa.eu/recruitment/working-for-enisa/faq-candidates (last visited on 8 Feburary 2020).
[49] ENISA, Decision No. MB/2013/15 of the Management Board of the European Union Agency for Network and Information Security Laying Down Rules on the Secondment of National Experts (SNE) to the Agency, 17 October 2013, art. 3, at 3, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/decision-no-mb201315-signed.pdf.
[50] ENISA, Public Procurement, https://www.enisa.europa.eu/procurement (last visited on 8 February 2020).

market strategy.[51] It results that the expertise of ENISA is important in this domain, both to be taken into account in fashioning the law, in addition to playing a role in the choice of standards and in the establishment and maintenance of a certification framework for various products and services. ENISA's power was increased through the adoption of the EU Cybersecurity Act in 2019,[52] and it now is to contribute to establishing and maintaining a certification framework through,[53] for example, preparing candidate certification schemes for adoption by the Commission through implementing acts.[54] ENISA will now contribute more generally to development and implementation of EU policy and law in the area of cybersecurity,[55] and to its implementation by Member States through expertise, advice and analyses, and 'soft law' such as opinions, guidelines, and best practices.[56] However, ENISA is a non-majoritarian body and stakeholder involvement in the main governing entities is minimal, with an advisory role through the ENISA Advisory Group. Furthermore, as an expert agency in a highly-scientific domain ENISA may have scientific legitimacy, but as has been noted in other agencies and sciences, this does not necessarily involve 'democratic legitimacy' or 'political responsibilities'.[57] It is there where administrative accountability, as made concrete in the foundational regulations of agencies and their governance provisions, plays a role. Weimar and Pisani speak of a control model of EU law as a model of 'administrative legitimation'. They note that, '[w]ide discretionary powers are seen as problematic, and need to be limited and controlled in order to maintain the democratic transmission between EU legislative commands and their administrative implementation.'[58] In this sense, coming back to the case at hand, we now investigate the level of power that ENISA exercises in connection with EU legislation.

[51] European Commission, 2015. A Digital Single Market for Europe – Analysis and Evidence SWD(2015) 100 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions [pdf]. European Commission, Brussels.
[52] Regulation (EU) 2019/881, [2019] OJ L151/15.
[53] *Id*., recital (48).
[54] 'The Commission, *on the basis of the candidate scheme prepared by ENISA*, should be empowered to adopt the European cybersecurity certification scheme by means of implementing acts' (emphasis added). *Id*., recital (84).
[55] *Id*., art. 4(2).
[56] *Id*., art. 5(2).
[57] Weimar, M. and Pisani, G., 2017. 'Expertise as Justification: The Contested Legitimation of the EU 'Risk Administration'' in *Regulating Risks in the European Union: The Co-production of Expert and Executive Power* (Weimer, M. and de Ruijter, A., eds., Hart Publishing), available at https://ssrn.com/abstract=2760791, at 4 (of the SSRN version).
[58] *Id*. at 7 (the authors also set forth a deliberative model of administrative legitimation, which is not developed here).

ENISA continues playing its part in fostering cooperation between the Member States and also between Member States and EU institutions, agencies and bodies, and now in facilitating efforts for the establishment and adoption of European and international standards for risk management and for 'measurable security of electronic products, systems, networks and services'.[59] We will first investigate ENISA's role in the context of data protection legislation, including the use of 'soft law' in this regard (1), prior to expanding this to electronic privacy (or 'eprivacy') legislation (2), NIS legislation (3), and, finally, data protection agency work on EU legislation (4), prior to concluding our discussion on EU legislation (5). This will lead us to a further discussions of ENISA and its accountability—in particular, in terms of ENISA's legal basis, the evolution of its mandate, the evolution of its governance structures, ,and political accountability.

4.1 Data Protection and 'Soft Law'

As the original founding legislative instrument for ENISA dates back only to 2004, Directive 95/46 (EC) (1995 Data Protection Directive)[60] precedes it by almost a decade and, therefore, makes no mention of the younger agency. Nonetheless, ENISA's role in relation to data protection has been recognized in the development of more recent legislative instruments, namely the General Data Protection Regulation.

ENISA played a role in the various consultations leading up to the Commission's proposal of the legislative instrument that was adopted, as amended, as Regulation (EU) 2016/679 ('General Data Protection Regulation', or 'GDPR'). As acknowledged in the explanatory memorandum to the Commission's 2012 draft GDPR, 'Dedicated workshops and seminars on specific issues were held throughout 2011. In January, ENISA organised a workshop on data breach notifications in Europe'.[61] Data breach notifications are new obligations for data controllers and data processors under Articles 33 and 34 of the GDPR.

Furthermore, several provisions of the GDPR make reference to 'appropriate technical and organisational measures', without defining the term. For example, this is the case in Article 25 on data protection by design and by default (although an approved data protection certification mechanism may be used as an element of proof of compliance). The security of processing provision (Article 32) requires 'appropriate technical and organisational measures

[59] Regulation (EU) 2019/881, supra note 52, recital (49).
[60] Directive 95/46 (EC), [1995] OJ L281/31.
[61] European Commission, 2012. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, at 3 (citations omitted).

to ensure a level of security appropriate to the risk', taking into account risk-level, costs of implementation, the state of the art, impact on the rights and freedoms of natural persons, and so on, although adherence to approved codes of conduct or certification mechanisms may be an element of proof of compliance. In addition, pseudonymisation and encryption, elements of cyber resilience, and regular cyber security assessment processes may be considered included within the term, as appropriate.[62]

Moreover, in deciding whether to impose an administrative fine or in deciding upon the administrative fine's amount, in the case of infringement of the GDPR, supervisory authorities are to give due regard to, *inter alia*, 'the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32' of the GDPR.[63]

It is in precisely these areas that ENISA has been working: creating guidelines, helping in sorting through standards, creating best practices, and so on. These may be considered 'soft law', which in certain cases may have legal effects, by supplementing legal instruments such as the GDPR. One definition of 'soft law' is '[r]ules of conduct that are laid down in instruments which have not be attributed legally binding force as such, but nevertheless may have certain (indirect) legal effects, and that are aimed at and may produce practical effects'[64]. There is a trend in the European Union to an increased level of soft law instruments.[65] One source contends that they constitute 10 per cent of EU law[66]. In an EU context the term is usually reserved to instruments of the European Union—that is of the EU institutions consisting primarily of the Council and the Commission, such as recommendations and opinions[67], although their use has grown to include instruments not mentioned in the TFEU such as notices, green and white papers, declarations, action programmes, codes of conduct and other acts.[68] Coman-Kund and Androne focus on soft law instruments adopted by the Commission 'because these seem to be most contested as to their legal nature and effects'[69].

---

[62] Regulation (EU) 2016/679, [2016] OJ L119/1, art. 32(1)(a)-(d).
[63] *Id*., art. 83(2)(d).
[64] Senden, L., 2004. *Soft Law in European Community Law* (Hart Publishing), at 112.
[65] Ferguš, V.R., 2014. 'The Growing Importance of Soft Law in the EU', 1(1) InterEU Law East 145-161, at 146.
[66] Ștefan, O., 2017. 'Soft Law and the Enforcement of EU Law' in *The Enforcement of EU Law and Values: Ensuring Member States' Compliance* (Jakab, A., and Kochenov, D., eds., Oxford University Press) 200-217, at 200 (citation omitted).
[67] See, for example, TFEU, supra note 23, art. 288.
[68] Ferguš, V.R., 2014, supra note 65, at 146.
[69] Coman-Kund, F. and Andone, C., 2019. 'European Commission's Soft Law Instruments: In-between Legally Binding and Non-binding Norms' in *Lawmaking in Multi-level Settings: Legislative Challenges in Federal*

This seems to fit well to the case of ENISA's work, which to a certain extent may be compared to the use of interpretative instruments by the Commission. Such instruments may be helpful in the application of EU legislation, not aiming 'at generating legal effects other than those ensuing from the underlying law itself'.[70] However, these may be seen as going further, filling in the blanks as it were, of 'vague or open' provisions of the law, itself.[71] While not intending to be an alternative to legislation (although they are of a general and normative nature), they complement it.[72] Ferguš speaks of the theory of graduated normativity, entailing a diversity of levels between legally-binding acts and non-legally-binding statements, and where soft law instruments have normative value and give rise to legal (and not just political) effects, thus influencing individuals, institutions, and Member States.[73] Furthermore, soft law has occasionally been used to interpret hard law in the courts[74], even though its use in court has been described as 'undesirable' and coming 'at the expense of legal certainty'[75].

Moreover, it has been recognized that is not only the principal EU institutions (the Council, the Commission and the Parliament) that issue soft law—EU agencies do as well.[76] Rocca and Eliantonio note that, 'Since soft law is not formally binding and, thus, does not create any rights or obligations, it seems to escape the limitations established by the *Meroni* judgement'[77], referring to a limitation excluding discretionary powers and general regualatory powers from what may be delegated to agencies by EU actors.[78] Dewar notes that ENISA helps its stakeholders deal with NIS problems through the publication of soft law, such as advice, assistance and guidelines.[79]

Senden identifies three main categories of soft law instruments. The first category includes preparatory and informative instruments, including Green and White Papers, action

---

Systems and the European Union 173-197 (Popelier, P., Xanthaki, H., Robinson, W., Tiago Silveira, J., and Uhlmann, F., eds., Nomos), at 174.

[70] Senden, L., 2004, supra note 64, at 143-144.

[71] *Id*., at 144 (referring to interpretative acts).

[72] *Id*., at 459.

[73] Ferguš, V.R., 2014, supra note 65, at 148.

[74] *Id*., at 151.

[75] Ștefan, O., 2017, supra note 66, at 202 (refernces omitted).

[76] Rocca, P. and Eliantonio, M., 2019, supra note 11, at 5-6, https://www.researchgate.net/publication/332464552_European_Union_Soft_Law_by_Agencies_an_Analysis_of_the_Legitimacy_of_their_Procedural_Frameworks.

[77] *Id*., at 6.

[78] *Id*., at 5.

[79] Dewar, R.S., 2017. 'The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern' in *Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security* 113-148 (O'Neill, M. and Swinton, K., eds., Cambridge Scholars Publishing), at 122.

programmes and informative communications.[80] Interpretative and decisional instruments form the second category. A third category consists of steering instruments, further divided into formal and non-formal steering instruments, which 'aim at establishing or giving further effect to Community objectives and policy, or related policy areas'.[81] Roughly speaking the first category corresponds to soft law's '*pre-law function*', the second its '*post-law function*', and the third, its '*para-law function*', used as an alternative to legislation.[82]

In a first example, in the area of privacy and data protection by design, covered by Article 25 of the GDPR, ENISA has published a report on privacy and data protection by design that may be used by data protection authorities 'as a reference of currently available technologies and methods' on privacy by design.[83] ENISA has also issued a study on privacy by design involving big data, focused mainly on technology, calling for the integration of privacy enhancing technologies as part of the practical implementation of data protection legal obligations.[84] Recourse to such post-law soft law tools is necessary to complement and add flexibility[85] to hard law instruments such as the GDPR.[86] In the case of the GDPR and ENISA, this is because soft law allows for standards used in the legislation to follow the rapid evolution of scientific technique, organisational procedures and threats in the area of cybersecurity. While the use of vague or open provisions of law such as in Article 25 may cause some head-scratching[87], without the flexibility that such provisions coupled with soft law allow, the legislation would contain requirements for security and privacy by design that would quickly become obsolete.

A second example concerns a draft Code of Conduct proposed by the Commission, where ENISA plays a guidance role. The final Draft Code of Conduct on privacy for mobile health

---

[80] Senden, L., 2004, supra note 64, at 118.
[81] *Id*., at 119.
[82] *Id*., at 120. In each case, Senden primarily focusses on instruments issued by the Commission or the Council.
[83] ENISA, 2014. Privacy and Data Protection by Design – from policy to engineering. December 2014. This report is cited as 'useful guidance in terms of what could constitute appropriate technical and organisational measures for the purpose of DPbD'. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G. & Leucci, S., 2018. 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR', *European Data Protection Law Review*, 4(2), 168-189, at 174.
[84] ENISA, 2015. Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. Final 1.0. Public. December 2015.
[85] Ferguš, V.R., 2014, supra note 65, p. 146 (noting the flexibility and differentiation of soft law, with the idea that this will lead to 'greater efficiency, flexibility, legitimacy and transparency of the EU legal order', although the author opines that this is 'questionable').
[86] Voss, W.G., 2019. 'Obstacles to Transatlantic Harmonization of Data Privacy Law in Context', U. Ill. J.L., Tech. & Pol'y, 2019(2), 405-463, at 457-458 (on the potential duration of the GDPR).
[87] See, for example, Hartzog, W., 2018. *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press), at 181 ('What does this obligation actually mean in practice? It's not entirely clear.').

applications has not yet been approved, as the most recent version was formally submitted to the Article 29 Data Protection Working Party (WP29) on 7 December 2017, and then rejected by WP29 on 11 April 2018.[88] The Commission seeks to have a the Code of Conduct revised in order then to submit it to the European Data Protection Board for formal approval.[89] In the current form of the final Draft Code of Conduct on privacy for mobile health applications, security measures necessary for such applications, pursuant to the data protection requirement 'to implement appropriate *technical and organizational measures* to protect personal data against accidental or unlawful destruction, loss, alteration, disclosure, access and other unlawful forms of processing' are discussed (emphasis added). In this respect, the draft Code of Conduct holds out ENISA documents as sources for guidance on secure smartphone app development and secure software development,[90] as well as with respect to technical mechanisms to implement privacy by design.[91] To the extent that guidance by ENISA is pointed to in a code of conduct, such guidance also participates in helping interpret and implement EU soft law, as well as EU legislation. It has been recognised that private rules such as codes of conduct play such latter role in data protection.[92]

Thus, ENISA has played a role in development of specific issues in data protection legislation, and its guidance provides missing elements for provisions of legislation that have been drafted in a vague manner. In such a way, we can say that it has helped participate in the creation of 'soft law', through what Senden would see as a contribution to the pre-law function (for example, through its contribution to the work on the GDPR), and most particularly, the post-law one (for example through reports, studies and other guidance referred to in a draft code of conduct and elsewhere).

4.2 Electronic Privacy

In our discussion of ENISA's role relating to legislation regarding privacy and electronic communications, we will first review this in connection with the ePrivacy Directive both

[88] European Commission, 2020. Privacy Code of Conduct on mobile health apps, https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps (last visited on 18 February 2020).
[89] *Id.*
[90] European Commission, 2017. Draft Code of Conduct on privacy for mobile health applications, 7 December 2017, notes 14 and 15, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125 (last visited on 18 February 2020), at 11.

[91] *Id.*, note 16, at 12.
[92] Hofmann, H.C.H., 2016, supra note 34, at 472 (at 15 in the version on SSRN), citing Directive 95/46 (EC), art. 27.

before and after its amendment (1), prior to considering this in the context of a proposed ePrivacy Regulation (2).

4.2.1 ePRIVACY DIRECTIVE

In Directive 2002/58/EC (ePrivacy Directive), adopted prior to the creation of ENISA, while security is addressed, the legislators chose to cross-reference the 1995 Data Protection Directive for security requirements in Recital 20: 'Security is appraised in the light of Article 17 of Directive 95/46/EC.' In the text of the ePrivacy Directive itself, vague references to requirements to 'take appropriate technical and organisational measures to safeguard security', are set out,[93] similarly to the case of the GDPR, discussed above, together with a reference to the 'state of the art', without giving any referential in order to evaluate these requirements. This is where guidelines, recommendations and best practices issued by ENISA may supplement the law, as we have seen above.

When the ePrivacy Directive was amended in 2009, ENISA was referred to directly in Article 2 of Directive 2009/136/EC (the 'Amending Directive") related to the ePrivacy Directive. Prior to the Commission adopting consistency 'technical implementing measures concerning the circumstances, format and procedures applicable' to new data beach notifications instituted by the Amending Directive, ENISA was given a right to be consulted (along with the WP29, an advisory group discussed below, and the European Data Protection Supervisor).[94] A draft Commission Decision implementing the personal data breach notification requirement, which was later turned into a regulation, included provisions defining which security measures are adequate to render data unintelligible (involving solutions such as encryption), were 'mainly based on the recommendations of ENISA.'[95]

In addition, ENISA and WP29 were to be consulted by the Commission before making comments or recommendations on proposed sanctions for infringement of the ePrivacy Directive to be added in member state implementing legislation, as communicated by national regulatory authorities, in particular to ensure compliance with the internal market. This follows a more general call for consultation of ENISA in the recitals of the Amending Directive:

[93] Directive 2002/58/EC, [2002] OJ L201/37, art. 4.
[94] Directive 2009/136/EC, [2009] OJ L337/11, art. 2(4)(c)(5).
[95] Article 29 Data Protection Working Party, 2012b. Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications (WP 197), at 8.

> When adopting implementing measures on security of processing, the Commission should consult all relevant European authorities and organisations (the European Network and Information Security Agency (ENISA) …), as well as all other relevant stakeholders, particularly in order to be informed of the best available technical and economic means of improving the implementation of [the ePrivacy Directive].[96]

Thus, ENISA plays an important consultative role in connection with security of processing aspects of the ePrivacy Directive, as well.

4.2.2 Proposed ePrivacy Regulation

Following a study on the implementation and effectiveness of the ePrivacy Directive and its compatibility with the GDPR, and public consultation, the Commission issued on 10 January 2017 a new proposed ePrivacy Regulation.[97] The European Commission acknowledges having relied on expert advice of ENISA, among other agencies, when drawing up the proposed ePrivacy Regulation.[98] For security requirements, Article 8(2)(b) of the proposed ePrivacy Regulation then made cross-reference to Article 32 of the GDPR,[99] rather than defining the requirements in the body of this instrument itself, and we have seen above the role of ENISA in helping supplement that regulation, through recommendations and guidelines. Although the proposed ePrivacy Regulation draft proposed by the Finnish presidency of the Council was rejected on 22 November 2019[100], work on a recast proposal is expected in 2020.

4.3 Network and Information Security (NIS) Directive and Cybersecurity

ENISA was consulted by the Commission prior to the proposal of the Network and Information Security Directive, and ENISA's 'continuous involvement' was seen as important element supporting the Commission and competent authorities' efforts 'to facilitate a

---

[96] Directive 2009/136/EC, supra note 94, recital (74).
[97] Voss, W.G., 2017. 'First the GDPR, Now the Proposed ePrivacy Regulation,' *Journal of Internet Law*, 21(1), 3-11.
[98] European Commission, 2017a. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.
[99] The 4 October 2019 draft of the ePrivacy Regulation contained this provision in its art. 8(2b). Council of the European Union, 2019. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003(COD), 12633/19, 4 October 2019, art. 8(2a), at 64, https://www.parlament.gv.at/PAKT/EU/XXVI/EU/07/70/EU_77024/imfname_10929175.pdf.
[100] Baker, J., 2019. 'How the ePrivacy Regulation talks failed … again', *iapp*, 26 November, https://iapp.org/news/a/how-the-eprivacy-regulation-failed-again/.

convergent implementation of the Directive across the EU'.[101] ENISA has a particularly central role to play in Directive (EC) 2016/1148 (NIS Directive). The NIS Directive has the objective of increasing network and information security,[102] and provides that Member States are to adopt a national NIS security strategy.[103] It establishes both security and notification requirements for operators of essential services (including in the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure)[104] and for digital service providers (online marketplace, online search engine, and cloud computing service providers).[105]

The NIS Directive creates a Cooperation Group, of which ENISA is a member, to further cooperation between Member States, particularly through the exchange of NIS information.[106] In this context, ENISA provides assistance in implementing policies and in analysing NIS security strategies and is involved in developing guidelines for 'sector-specific criteria for determining the significance of the impact of an incident', among other responsibilities.[107] When the Commission adopts implementing acts relating to procedural arrangements necessary for the Cooperation Group's functioning, or on the security requirements for digital service providers, 'the Commission should take the utmost account of the opinion of ENISA.'[108]

The Commission or the Member States may consult ENISA regarding the application of the NIS Directive, and the agency is to provide them with expertise and advice.[109] It coordinates simulated real-time cyber incident scenario exercises as a tool for testing and drawing up recommendations for improving incident-handling.[110] ENISA is also to collaborate with Member States on the development of advice and guidelines regarding technical areas to be considered in connection with the use of technology, standards and specifications, relating to the security of networks and information systems.[111]

---

[101] European Commission, 2013. 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 COM(2013) 48 final.
[102] Directive (EC) 2016/1148, [2016] OJ L194/1, art. 1(1).
[103] *Id*., art. 7(1).
[104] *Id*., art. 14.
[105] *Id*., art. 16.
[106] *Id*., art. 11(1)-(2).
[107] *Id*., recital (38).
[108] *Id*., recital (69).
[109] *Id*., recital (36).
[110] *Id*., recital (42).
[111] *Id*., art. 19(2).

Furthermore, the importance of the role of ENISA in NIS and more generally cybersecurity has recently been highlighted by which the Council invited ENISA, Europol and Eurojust,

- to continue strengthening their cooperation in the fight against cybercrime, both among themselves and with other relevant stakeholders, including the CSIRTs community, Interpol, the private sector and academia ensuring synergies and complementarities, in accordance with their respective mandates and competences.
- to contribute jointly with Member States a coordinated approach for EU law enforcement response to large-scale cyber-incidents and crises to complement the procedures outlined in the relevant frameworks (citation omitted).[112]

Thus, we see that ENISA's role is central in advising the Commission and Member States in the area of NIS security and in providing guidelines, and otherwise in ensuring a coherent approach to cybersecurity throughout the European Union.

4.4 Data Protection Agency Work Regarding EU Legislation

In addition, the work of ENISA has been considered by the Article 29 Data Protection Working Party (WP29), a European advisory group established under Article 29 of the 1995 Data Protection Directive, which has now been replaced by the European Data Protection Board (EDPB), in its deliberations on various issues related to European legislation.

For example, in connection with the Commission's recommendation that Member States 'adopt and apply a template for a data protection impact assessment ('DPIA Template'), which should be developed by the Commission and submitted to the Working Party on the protection of individuals with regard to the processing of personal data (WP29) for its opinion within 12 months of publication of the Commission Recommendation', WP29 found that the proposed DPIA Template often confused risks and threats, and referred to ENISA's threat landscape.[113] About the security requirements applicable to smartphone apps, WP29 cites ENISA guidelines as among the 'publicly available guidelines regarding the security of mobile apps'.[114]

Furthermore, WP29 cooperates with ENISA on various issues. For example, WP29 and ENISA worked together on developing a harmonized European personal data breach severity assessment methodology, following the introduction of data breach notifications under the

[112] Council, 2017. Draft Council conclusions on the Joint Communication to the EP and the Council: Resilience, Deterrence and defence: Building strong cybersecurity for the EU, 20 November 2017, 14435/17.
[113] Article 29 Data Protection Working Party, 2013b. Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205).
[114] Article 29 Data Protection Working Party, 2013a. Opinion 02/2013 on apps on smart devices (WP 202).

ePrivacy Directive, as amended by the Amending Directive.[115] WP29 stated that such joint work on severity assessment should be incorporated in the breach notification form under the GDPR, as well.[116]

4.5 EU Legislation and the Role of ENISA: Conclusion

We have seen that ENISA has played a certain role in the development of EU law in the areas of data protection, electronic privacy, and cybersecurity, through information providing and that it also may help 'complete' the law, by allowing a way to gauge compliance with security requirements of the law. One may see that because of the lack of expertise of the lawmaker, and as a means to allow for changes in the state of the art over time, aspects of security requirements have in essence been delegated to the standard-makers and to the agency responsible for sifting through these standards – ENISA – through their non-inclusion in the legislative instruments themselves. Thus, ENISA's role must be evaluated in the light of this power.

.

5. An Early Challenge to ENISA's Legal Basis

Early on in ENISA's existence, in *United Kingdom v Parliament and Council,* the United Kingdom of Great Britain and Northern Ireland applied to the European Court of Justice (ECJ) for annulment of the ENISA Regulation on the grounds that it alleged that then Article 95 EC (now Article 114 TFEU[117]) did: 'not provide an appropriate legal basis for adoption of that regulation. The power conferred on the Community legislature by Article 95 EC is the power to harmonise national laws and not one which is aimed at setting up Community bodies and conferring tasks on such bodies.'[118] The United Kingdom was the only Member State that voted against the ENISA Regulation, and this on the same grounds.[119]

The import of this argument was that, while the ENISA Regulation was adopted under one provision of the EC Treaty (Article 95 EC, which refers to the procedure in Article 251 EC[120]) by qualified majority vote of the Council through the co-decision procedure with the

[115] Article 29 Data Protection Working Party, 2012b, supra note 86.
[116] Article 29 Data Protection Working Party, 2012a. Opinion 01/2012 on the data protection reform proposals (WP 191).
[117] TFEU, supra note 23, art. 114.
[118] Case C-217/04, 2006. Judgment of the Court (Grand Chamber), 2 May 2006, United Kingdom v Parliament and Council, para. 11.
[119] Case C-217/04, 2005. Opinion of Advocate General Kokott, 22 September 2005, United Kingdom v Parliament and Council, para. 50.
[120] The corresponding provision of the TFEU, now referring to the "ordinary legislative procedure," is art. 294.

Parliament, it should have been adopted by unanimous vote of the Council on proposal of the Commission and after consulting the Parliament instead (then Article 308 EC, now Article 352 TFEU[121]).[122] The ECJ found that the ENISA Regulation was rightly based on Article 95 EC and therefore dismissed the action, but it is interesting to note the ECJ's discussion of the role of ENISA: in the context of the risk of a 'heterogeneous application of the technical requirements laid down in [Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services] and the specific directives', the EC legislature 'was entitled to consider that the opinion of an independent authority providing technical advice at the request of the Commission and the Member States might facilitate the transposition of the directives at issue into the laws of the Member States and the implementation of those directives at national level.'[123] The ECJ also pointed out that the mandate of ENISA was limited in time to five years and this allowed an evaluation of the effectiveness of ENISA before 'making a decision as to the fate' of that agency.

The ECJ's emphasis on the technical nature of the work of ENISA echoes Recital 3 of the preamble to the ENISA Regulation, cited by the Advocate General in her opinion in *United Kingdom v Parliament and Council*:

> 4. The preamble to the ENISA Regulation explains why it is necessary to set up [ENISA]. Recital 3 in the preamble describes the problem:
>
> 'The technical complexity of networks and information systems, the variety of products and services that are interconnected, and the huge number of private and public actors that bear their own responsibility risk undermining the smooth functioning of the Internal Market.'[124]

It should be noted that the ECJ did not follow the opinion of the Advocate General; the latter was for an annulment of the ENISA Regulation, stating: 'Since the ENISA Regulation does not adequately define ENISA's contribution to the approximation of laws and none of the other views on the applicability of Article 95(1) prevails, the ENISA Regulation must in any event be annulled.'[125]

[121] TFEU, supra note 23, art. 352. Note that this corresponding article of the TFEU requires not just consultation with the European Parliament, but its consent.
[122] *See*, *e.g.*, Andoura, S., and Timmerman, P., 2008. 'Governance of the EU: The Reform Debate on European Agencies Reignited,' EPIN Working Paper No. 19, October 2008, at 8.
[123] Case C-217/04, 2006, supra note 118, paras. 63-64.
[124] Case C-217/04, 2005, supra note 119, para. 4.
[125] *Id*., para. 46.

The submissions and claims of the parties, contained in the ECJ's opinion, regarding the role of ENISA are enlightening: the ECJ cited both the United Kingdom submission that ENISA 'must limit itself to providing non-binding advice', and the Parliament's claims on the limited role of that agency:

> According to the Parliament, the functions of [ENISA] are relatively modest in that they do not include the power to adopt 'standards'. The provision of advice by a single authoritative source of expertise at the European level contributes to the adoption of common positions in situations where the Community and the national bodies cannot run the risk of receiving conflicting technical advice. The various forms of cooperation promoted by [ENISA] also facilitate the approximation of market conditions and the adoption by the Member States of measures which tackle information problems.[126]

Thus, while ENISA has had a limited role, which we have already noted may be greater than it seems, it has acted in a technically complex field, and came under fire from the start. While questions of accountability were addressed in part through governance structures, ENISA first had to survive a crucial test of the legitimacy of its foundational regulation, and the ECJ's ruling confirmed the broad scope of harmonisation of national laws measures allowed under the internal market legal basis.[127] In summary, 'ENISA has been accepted by the CJEU, because this agency was creted for adopting non-binding supporting and framework measures under the condition that its tasks are closely related to the subject-matter of the relevant harmonising measures[128].

6. The Evolution of ENISA's Mandate

ENISA's original mandate of five years[129] was extended a first time until 13 March 2012 by an amending regulation.[130] In 2010, the Commission found that it was necessary to revise provisions regarding ENISA, and cited earlier studies indicating that there was a need to modernise, reinforce, and further develop ENISA 'to support the Commission and Member States in bridging the gap between technology and policy, serving as the Union centre of expertise in NIS matters.'[131] This was seen as especially important because of the crucial role of ICTs in the European economy and society, highlighted by a Council Resolution called for

[126] Case C-217/04, 2006, supra note 118, para. 27.
[127] Vos, E., 2018, supra note 6, at 26-27 (Vos refers to the 'lenient case law' of the ECJ, indicating the Article 114 will often be the proper legal basis for EU agencies).
[128] Coman-Kund, F., 2018, supra note 32, at 34.
[129] ENISA's limited time character was an exception to the general rule that agencies (other than "agencies classified as executive agencies by the Commission") were given a permanent character. Andoura and Timmerman, 2008, supra note 122, at 9.
[130] Regulation (EC) No 1007/2008, [2008] OJ L293/1, art. 1.
[131] European Commission, 2010b. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration COM(2010) 520 final, at 3.

a 'reinforced and flexible mandate' for ENISA.[132] A renewed ENISA was also called for as part of the Digital Agenda.[133] At the same time, it was felt that much debate would be required in order to revise provisions regarding ENISA so the Commission decided to ask for extension of the duration of ENISA for eighteen months to allow time for the debate. The latter was achieved through Regulation (EU) No 580/2011, extending ENISA's mandate until 13 September 2013.[134]

In May 2013, Regulation (EU) No 526/2013 (2013 ENISA Regulation) was adopted, extending the mandate of ENISA until 18 June 2020.[135] Later, Regulation (EU) 2019/881 (EU Cybersecurity Act) made ENISA's mandate indefinite as of 27 June 2019,[136] subject to evaluation and review every five years by the Commission, starting by 28 June 2024, which may include the proposal of amendment of the EU Cybersecurity Act to modify ENISA's mandate.[137] This periodic evaluation and review procedure may be considered an accountability mechanism, although the fact that ENISA's mandate is now otherwise 'permanent' gives more reason to focus on its governance structures, as another way to ensure accountability.

7. The Evolution of ENISA's Governing Structures: One Way to Obtain Accountability

We now turn to an analysis of ENISA's evolving governance structures. This exercise will highlight the relatively limited role for ENISA foreseen by the legislature, its classical EU regulatory agency governing structure, as well as the technically complex area in which ENISA was to intervene. Governing structures are one way used to help ensure what Curtin refers to as 'administrative' accountability, or the accountability between 'elected politicians and bureaucrats', which is the narrower category of accountability.[138] This kind of accountability includes ex ante control in the form of the original terms of the delegation of power or mandate (although this area may be placed in either the category of legal or political accountability, instead), as well as ongoing control in the lack of independence in terms of

[132] Council, 2009. Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, [2009] OJ C321/1, at 4.
[133] European Commission, 2010a. 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) 245 final, at 17.
[134] Regulation (EU) No 580/2011, [2011] OJ L165/3, art. 1.
[135] Regulation (EU) No 526/2013, [2013] OJ L165/41, art. 36.
[136] Regulation (EU) 2019/881, supra note 52, art. 68(4).
[137] *Id*., art. 67(1).
[138] Curtin, D., supra note 13, at 247-248.

decision-making, and ex post control, through annual reports and budget discharges, etc.[139] It is concerned with controlling delegated powers,[140] and is helpful in the context of ensuring transparency, controlling the use of EU funds, and guaranteeing proper governance. The ENISA Regulation remained the fundamental regulation of ENISA until repealed and replaced by the 2013 ENISA Regulation, which itself was repealed and replaced by the EU Cybersecurity Act in 2019.

Under the ENISA Regulation, which contained the original terms of delegation of power to the agency, ENISA was formed as a body of the European Community, having legal personality, and its operations were subject to the supervision of the Ombudsman. Its accounts were sent to the EU institutions, was subject to observations of the Court of Auditors, and the implementation of its budget required a discharge from the European Parliament. The bodies of ENISA under the ENISA Regulation consisted of a Management Board, an Executive Director, and a Permanent Stakeholder Group. The 2013 ENISA Regulation retained the original governing bodies (with some changes) and added an Executive Board. All of these governance provisions applied to an agency with relatively little staff, as discussed in paragraph 6 below. In terms of governance structures, the EU Cybersecurity Act no longer refers to a Permanent Stakeholder Group, but to an ENISA Advisory Group and a National Liaison Officers Network, instead.[141] Each of these elements is detailed, prior to discussing ENISA's current status.

7.1 The Management Board

Under the ENISA Regulation, the Management Board was made up of representatives of Member States (one each), the Commission (three), and three non-voting representatives proposed by the Commission and appointed by the Council representing, respectively, the information and communication technologies (ICT) industry, consumer groups, and academic experts in NIS.[142] Board members were appointed based on their experience and expertise in the NIS field.[143] Initially, we notice the preponderant weight of the Member States in this governance structure, and the lack of vote for stakeholders outside of the EU institutions. The Management Board elected a Chairperson and a Deputy Chairperson from its membership for a renewable two-and-a-half-year period.[144] The Commission proposed rules of procedure for

[139] *Id*., at 250.
[140] *Id*., at 247.
[141] Regulation (EU) No 2019/881, supra note 52, art. 13.
[142] Regulation (EC) No 460/2004, supra note 8, art. 6(1).
[143] *Id*., art. 6(2).
[144] *Id*., art. 6(3).

adoption by the Management Board, and a two-thirds majority vote of the Management Board was necessary for their adoption, as well as for the adoption of ENISA's rules of operation, the budget, the annual work programme, and the appointment and removal of the Executive Director. Otherwise, voting was by a majority of voting members, unless provided differently.[145] Ordinary meetings were to be held twice a year, with extraordinary meetings convened at the request of the Chairperson or at least a third of the voting membership.[146]

The Management Board defined the general orientation for the operation of ENISA and ensures consistency of work with Member State and Community-level activities. The Management Board also adopted annual work programmes, ensuring that they are consistent with ENISA's scope, objectives and tasks as well as Community NIS legislative and policy priorities. Furthermore, the Management Board adopted an annual general report of ENISA's activities and, after consulting with the Commission, financial rules applicable to ENISA, which were not to depart from those set out in Commission Regulation (EC, Euratom) No 2343/2002,[147] without the Commission's prior consent.[148]

With the adoption of the 2013 ENISA Regulation, the rules of procedure of ENISA were no longer proposed by the Commission; the Management Board had to consult with the Commission before adopting them, instead.[149] Thus, the EU executive gave up a certain degree of formal control over a governance structure essentially controlled by Member State representatives. In addition, the composition of the Management Board was modified to decrease the Commission representatives to two,[150] and the former non-voting members from stakeholders were no longer included among its members. The latter change was given the following justification: 'Since there is provision for ample representation of stakeholders in the Permanent Stakeholders Group, and that group is to be consulted in particular regarding the draft Work Programme, there is no longer any need to provide for representation of stakeholders in the Management Board.'[151] This move, it may be argued, hindered accountability to stakeholders outside of the EU institutions (more an element of political accountability), while at the same time also reducing control of the executive.

[145] *Id*., art. 6(4).
[146] *Id*., art 6(5).
[147] Commission Regulation (EC, Euratom) No 2343/2002, [2002] OJ L357/72.
[148] Regulation (EC) No 460/2004, supra note 8, art. 6.
[149] Regulation (EU) No 526/2013, supra note 135, art. 5(10).
[150] *Id*., art 6(1).
[151] *Id*., recital (48).

Furthermore, the requirement of a two-thirds majority was extended to the designation of the Chairperson of the Management Board,[152] in addition to the existing cases. This move can be seen as further ensuring Member State control in the agency. The renewable term of the Chairperson was extended to three years,[153] and the term of office of members of the Management Board was set at four years, which was renewable.[154] The Management Board was to adopt an anti-fraud strategy[155] (and a provision allowing the Court of Auditors to have the power of audit over grant beneficiaries, contractors and subcontractors who have received EU funds has been added[156]), and rules for the prevention and management of conflicts of interest,[157] among other new responsibilities. The required frequency of meetings of the Management Board was decreased to at least once a year.[158] No provision was made in the 2013 ENISA Regulation for Permanent Stakeholders Group members to attend Management Board meetings.

The Commission is represented on the Management Board by its Deputy Director-General, Director (acting) for Digital Society, Trust and Cybersecurity, and by the Chief Information Security Officer of DG DIGIT.[159] Most Member State representatives on the Management Board come from information security/cybersecurity divisions of government ministries, with representatives of ministries of transportation and communication data, of digital governance, of the interior, of economic development, of defence, of security and justice, and of public administration included. Other representatives come from specific NIS or communications regulatory bodies (including independent agencies) or computer emergency response teams (CERTs). One Member State is represented by its chief information officer. Surprisingly for an expert agency, perhaps, only one Member State (Poland) is represented by someone coming from what is described as a national research institute (Research and Academic Computer Network (NASK)).[160] Thus, industry, academia and research (for the most part), data protection authorities, consumer organisations and standardisation agencies are all

[152] *Id*., art. 9(2).
[153] *Id*., art. 7(1).
[154] *Id*., art. 6(4).
[155] *Id*., art. 5(4).
[156] *Id*., art. 20(2).
[157] *Id*., art. 5(6).
[158] *Id*., art. 8(2).
[159] *Id*.
[160] ENISA, List of ENISA Management Board Representatives and Alternates, Status 1 February 2020, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/MBMemberAlternate.pdf (last visited on 3 February 2020).

stakeholders absent from the Management Board, although present in the Advisory Group to varying extents.

The EU Cybersecurity Act lengthened the term of office of the Chairperson of the Management Board to four years, renewable once.[161] The frequency of ordinary meetings of the Management Board were increased to twice a year.[162] Unlike the Permanent Stakeholders Group members under the 2013 ENISA Regulation, under the EU Cybersecurity Act members of the ENISA Advisory Group may participate (without voting rights) in meetings of the Management Board by invitation of the Chairperson.[163] Although an improvement over the 2013 ENISA Regulation, the fact that Advisory Group must be invited to attend meetings and will have no vote there may still indicate a deficit of political accountability at a time when ENISA is receiving greater powers, in that stakeholders are not directly included at meetings where the agency's decisions are being made, except through invitation, and when invited, have no vote.

7.2 The Executive Director

Under the ENISA Regulation, the Executive Director represented ENISA[164] and managed ENISA and was independent in the performance of his or her duties. He or she was appointed by the Management Board for an up to five-year term, on proposal of the Commission, following an open competition, based on his or her merit and administrative and management skills and competence and experience relative to NIS. He or she chaired the Permanent Stakeholder Group[165] and participated in a non-voting capacity at meetings of the Management Board and provided the Secretariat.[166] Under the 2013 ENISA Regulation, the Executive Director's term was set at five years, extendable once for no more than five years, by the Management Board, acting on a proposal from the Commission, after obtaining the European Parliament's views.[167] The Executive Director now chairs the Advisory Group—the successor to the Permanent Stakeholder Group[168], which allows a link between this group and the other instances of the agency such as the Management Board, but also may create a concern about the independence of the body, as not having proper distance and independence

[161] Regulation (EU) No 2019/881, supra note 52, art. 16.
[162] *Id*., art. 17(2).
[163] *Id*. art. 17(4).
[164] Regulation (EC) No 460/2004, supra note 8, art. 18(3).
[165] *Id*., art. 7.
[166] *Id*., art. 6(5).
[167] *Id*., arts. 5 and 24.
[168] Regulation (EU) No 2019/881, supra note 52, art. 21(3).

between the Advisory Group and the ENISA management that it advises. Lenstsch and Weingart theorise that there should be distance and mutual independence between advisers and the advised to 'avoid the mixing of particularistic interests and scientific judgements' so as not to lose credibility, authority and its legitimating function.[169]

The Executive Director position has been held by Mr. Juhan Lepassaar—who came to ENISA after six years in the European Commission, which followed his work at the Estonian Government Office—since 16 October 2019.[170]

7.3 The Permanent Stakeholder Group

Under the ENISA Regulation, the Permanent Stakeholder Group was composed of experts representing stakeholder groups (ICT industry, consumer groups, and academic experts in NIS).[171] It is important that these different groups be included, as ensuring pluralism of the technical body. The value of this pluralism is highlighted by Lentsch and Weingart: 'Different disciplines and advisers must be represented in the advisory process, adequately reflecting the topics in question. A plurality of perspectives, theories and methods safeguard the adequacy of the knowledge and the trust in it.'[172]

ENISA's internal rules of operation were to specify the number and the composition of the membership,[173] who were to serve for two-and-a-half-year terms and were not to be members of the Management Board. The Executive Director was to establish and chair the group.[174] Representatives of the Commission could attend meetings of the group and participate in its work.[175] The group could advise the Executive Director in his or performance of duties and in drawing up ENISA's work programme and could help ensure communication with stakeholders on issues related to the work programme.[176]

Under the 2013 ENISA Regulation the Permanent Stakeholders Group could be composed of representatives from additional categories of stakeholders such as providers of electronic communications networks or services available to the public, representatives of national

---

[169] Lentsch, J. and Weingart, P., 2011. 'Introduction: the quest for quality as a challenge to scientific policy advice: an overdue debate?' (Chapter 1) in *The Politics of Scientific Advice: Institutional Design for Quality Assurance* 3-18 (Lentsch, J. and Weingart, P., eds., Cambridge University Press), at 15.
[170] ENISA, The Executive Director, https://www.enisa.europa.eu/about-enisa/structure-organization/executive-director (last visited on 3 February 2020).
[171] Regulation (EC) No 460/2004, supra note 8, art. 8(1).
[172] Lentsch, J. and Weingart, P., 2011, supra note 164, at 15.
[173] Regulation (EC) No 460/2004, supra note 8, art. 8(2).
[174] *Id*., art. 8(3).
[175] *Id*., art. 8(4).
[176] *Id*., art. 8(5).

regulatory agencies notified under Directive 2002/21/EC, and law enforcement and privacy protection authorities.[177] In practice, in addition to representatives nominated by the Body of European Regulators for Electronic Communications (BEREC), the Article 29 Data Protection Working Party, and the European Union Agency for Law Enforcement Cooperation, there were certain Permanent Stakeholder Group members appointed 'ad personam'. The actual composition of such category of members on 3 November 2017 was: five members from academia; nineteen from industry (including members from Airbus, Continental Tires, Ebay, Google, Nokia, STMicroelectronics, SWIFT, and others), one from a consumer group (BEUC), and five from other sectors (such as standardisation and rating agencies, amongst others).[178] If we consider that BEUC represents the public, all main ENISA target stakeholders groups identified by Parliament report, were represented on the Permanent Stakeholder Group or the Management Board:

> 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.[179]

In the EU Cybersecurity Act, this structure was replaced by an ENISA Advisory Group,[180] detailed in Section 5 below.

7.4 The Executive Board: A Contribution of the 2013 ENISA Regulation

The reason given for the creation of a new governing body – the Executive Board – was to 'enable the Management Board to focus on issues of strategic importance' in an attempt to simplify and strengthen the organisational structure of ENISA to allow greater efficiency and effectiveness.[181] The Executive Board was intended to assist the Management Board by preparing decisions to be adopted by the latter 'on administrative and budgetary matters only', and by assisting and advising the Executive Director in implementing these decisions, and by

[177] Regulation (EU) No 526/2013, supra note 135, art. 12(1).
[178] ENISA, 2017. The Permanent Stakeholder's Group, Term of office: 1st November 2017-1st May 2020, Status 3 November 2017.
[179] European Parliament, Briefing, Implementation Appraisal, 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, May 2017, at 3, https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/603231/EPRS_BRI(2017)603231_EN.pdf.
[180] Regulation (EU) 2019/881, supra note 52, art. 21.
[181] *Id*., recital (42).

following up findings and recommendations resulting from investigations of the European Anti-Fraud Office (OLAF), and various internal and external audit reports and evaluations. The renewable term of office for members of the Executive Board was four years, and their number five, appointed from the membership of the Management Board amongst whom the Chairperson of the latter (who may also serve as the former's chair), and one of the Commission's representatives. Meetings were to be held at least once every three months and the chair could convene additional meetings at the request of its members.[182] This structure was continued in the EU Cybersecurity Act, virtually unchanged, with the exception of a proviso that has been added allowing the Executive Board to take certain 'provisional decisions' in the place of the Management Board, especially on administrative matters, on an urgent basis, to be followed up by a ratification (or not) of the latter body.[183] Its current composition includes a representative from the European Commission (Deputy Director-General, Director (acting) for Digital Society, Trust and Cybersecurity); as well as four from Member States: the Chair of the Management Board (who comes from France's ANSSI), the Head NCSC and Deputy director Cyber Security from the Netherlands' Ministry of Security and Justice, the Austrian Chief Information Officer, and the Deputy Head of Poland's Research and Academic Computer Network (NASK).[184]

7.5 The ENISA Advisory Group, Stakeholder Cybersecurity Certification Group and the National Liaison Officers Network: Modifications Made by the EU Cybersecurity Act

The EU Cybersecurity Act was meant to grant a much greater role for ENISA in cybersecurity in Europe.[185] It provides for the establishment of an ENISA Advisory Group, a Stakeholder Cybersecurity Certification Group and a National Liaison Officers Network. The first of these groups, the ENISA Advisory Group, may be seen as a successor to the Permanent Stakeholders Group,[186] while the latter two may be seen as having been created relating to the expansion of ENISA's role into certification and an increase in its cooperation with Member

[182] *Id*., art. 10.
[183] Regulation (EU) No 2019/881, supra note 52, art. 19.
[184] ENISA, List of ENISA Executive Board Representatives and Alternates, Status 21 January 2020, https://www.enisa.europa.eu/about-enisa/structure-organization/executive-board/enisa-executive-board-members (last visited on 3 February 2020).
[185] European Commission, 2017b. 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) 477 final.
[186] Indeed, ENISA refers to its Advisory Group as the 'former Permanent Stakeholder's Group'. ENISA, 2019. The Advisory Group (former Permanent Stakeholder's Group). 26 June 2019.

States. Certain of the provisions of the EU Cybersecurity Act with respect to certification have a delayed entry into force date of 28 June 2021.[187]

Similar to the former Permanent Stakeholders Group, the ENISA Advisory Group is proposed by the Executive Director. The Management Board then acts upon this proposal. The ENISA Advisory Group's membership may come from diverse sources, much like the Permanent Stakeholders Group following the modifications made by the 2013 ENISA Regulation. In the case of the ENISA Advisory Group, these may include relevant stakeholders such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, cybersecurity academic experts, representatives of competent authorities notified under Directive (EU) 2018/1972, European standardisation organisations, law enforcement and data protection supervisory authorities. Furthermore, it is to reflect gender, geographical and stakeholder group balance.[188] However, as its name suggests, it only plays an advisory role, which does not extend to the cybersecurity certification framework.[189] Its composition on 26 June 2019 included nominated representatives of BEREC, Europol, and the successor to the Article 29 Data Protection Working Party—the European Data Protection Board (EDPB). In addition, there were five representatives from academia, eighteen from industry, one from a consumer group, and five from other sectors. These consisted of the same persons as on the Permanent Stakeholders' Group mentioned in Section 3 above, with the following exceptions, all involving representatives from industry: the representative from Rohde & Schwartz Cybersecurity, who had gone to work for a German region, instead, left the Group; the representative of Philips left the Group; and a new representative from Cap Gemini joined the Group.[190]

While the representation of various stakeholders on the Advisory Group is laudable, the failure to automatically include certain members on the Management Board may be seen as a weakness. Thus, in the context when the role of ENISA is increasing, paradoxically stakeholders have less access to the centre of decision-making than in the original ENISA Regulation.

---

[187] Regulation (EU) No 2019/881, supra note 52, art. 69(2).
[188] *Id*., art. 21(1).
[189] Id., art. 21(5)
[190] ENISA, 2019. The Advisory Group (former Permanent Stakeholder's Group), Term of office: 1st November 2017-1st May 2020, Status 26 June 2019, https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group/members/ag-composition-2017-2020/view.

7.6 ENISA'S BUDGET AND STAFFING

ENISA's budget has been relatively small throughout its short history, when compared to other agencies. Furthermore, its staffing has been small. ENISA's budget remained under €10 million from 2005 through 2014 (see Table 1 below). The highest annual increase in its budget occurred in the most recent year—2019—which is the year when the EU Cybersecurity Act was adopted and political aims were to strengthen ENISA. In that year, the budget increased €5,483,952 or by nearly 50% (47.9%) over the prior year. Its budgeted temporary agent staff remained constant from 2006 through 2011 at 44, increasing by less than 10% during the following period through 2018 to 47. It was only in the last year that, in at the same time that its budget increased significantly, ENISA temporary agent staff increased by over a quarter (25.53%). The EU website shows that, from a numerical perspective, ENISA has been a small agency, with 65 total staff members.[191] By contrast, EASA, which is an agency that has 'the power not only to assist the Commission in the exercise of rulemaking powers but also to directly adopt technical rules'[192] (which is not the case for ENISA today) had a budget in 2019 of €103,214,000,[193] more than six times that of ENISA's highest budget amount. EASA has a staff of 840 members,[194] nearly thirteen times that of ENISA. However, the basic governance of EASA (except for the latter's Board of Appeal)[195] is similar (but not identical) to that of ENISA, making one wonder if the administrative accountability provisions for ENISA were not, at least for the period prior to 2019 and the EU Cybersecurity Act, excessive, in the sense attributed to it by Busuioc. Indeed, a one-size fits all strategy for oversight merely results in agencies spending more time on administrative tasks related to audit requirements.[196] This pleads for a more customised set

[191] European Union, 2019a. European Union Agency for Network and Information Security (ENISA): Overview, https://europa.eu/european-union/about-eu/agencies/enisa_en (last visited on 5 October 2019).
[192] Chiti, E., 2013. 'European Agencies' Rulemaking: Powers, Procedures and Asessment', *European Law Journal*, 19(1), 93-110, at 97. EASA has been described as 'both a decision-making and a quasi-rulemaking agency'. Saurer, J., 2009. 'The Accountability of Supernational Administration: The Case of European Union Agencies', *American University International Law Review*, 24(3), 429-488, at 464.
[193] EASA, 2019. *Annex 1: 2019 First Amending Budget – Detailed Table*, https://www.easa.europa.eu/sites/default/files/dfu/EASA%20MB%20Decision%2006-2019%20Annex%201%20-%201st%20amending%20budget%20detailed%20table.pdf.
[194] European Union, 2019b. European Union Aviation Safety Agency (EASA): Overview, https://europa.eu/european-union/about-eu/agencies/easa_en (last visited on 6 October 2019).
[195] Regulation (EU) 2018/1139, [2018] OJ L212/1, arts. 94-106. Chiti also refers to EASA having a 'rulemaking directorate', which is absent in ENISA. Chiti, E., 2013, supra note 187, at 97.
[196] 'First, as Busuioc notes, agencies spend on average 30 per cent of their staff resources on administrative tasks—and some more then 50 per cent—due to extensive audit requirements'. Eriksen, A., 2019. 'Agency accountability: Management of expectatations or answerability to mandate?', TARN Working Paper 02/2019, at 7.

of accountability rules for agencies such as ENISA, contrary to the Common Approach on EU Agencies.

Table 1: ENISA Budget and Temporary Agent Posts

Year	ENISA Annual Budget (in €)	Staff Temporary Agent Posts
2005	6,800,000	38
2006	6,940,080	44 (38 + 6 filled during year)
2007	8,416,928	44
2008	8,355,024	44
2009	8,117,200	44
2010	8,113,988	44
2011	8,102,920	44
2012	8,550,149	47
2013	8,549,553	47
2014	9,086,354	48
2015	10,095,949	48
2016	11,060,564	48
2017	11,175,225	48
2018	11,449,000	47
2019	16,932,952	59

Source: ENISA[197]

7.7 The Evolution of ENISA's Governing Structures: Conclusion

We have investigated the past and present basis for, and governance of ENISA. We have seen that, following a relevant set of taxonomies,[198] ENISA is, from a functional perspective, an agency with tasks related to expertise, and information and cooperation. Although under the EU Cybersecurity Act it will now contribute to the adoption of a certification framework, it is not today involved in providing services such as registration and certification. Furthermore, it does not supervise, inspect, or enforce, nor does it execute EU programmes. As we have seen, ENISA is a small agency. This fact was at the root of criticism of the Cybersecurity Act proposal by the head of France's cybersecurity agency, the *Agence*

[197] ENISA, 2019. *Annual Budgets*, https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets (last visited on 30 January 2020). Where there was an amended budget amount for a certain year, that amended amount was retained for this table. Decimals have been rounded to the nearest Euro, with 51 cents and more being rounded up. Certain years include a contribution from the EFTA countries, a subsidy from the Greek Government for the rent of the offices of ENISA in Greece (set to a maximum of € 640,000) (in the latter case, for the periods from 2013 through 2019, described in the earlier years as a 'subsidy from the host member State covering the hosting needs of the Agency'), and the interest on cash deposits. For a comparative view, to show just how low ENISA's budget is, Carrapico and Barrinha contrast ENISA's 2016 budget of roughly €11 million to the cybersecurity budget of the Pentagon, which requested USD 3.2 billion of cybersecurity funding, during the period when reported by those authors. Carrapico, H. & Barrinha, A., 2017, supra note 38, at 1264.

[198] Vos, E., 2014. 'European Agencies and the Composite EU Executive,' in *European Agencies in between Institutions and Member States* (M. Everson, C. Monda, & E. Vos, eds., Wolters Kluwer Law & Business), at 26, at 17-23. In one typology of power, ENISA is arranged in the information providing agencies category, the least powerful of the categories. Busuioc, E.M., 2013, supra note 1, at 38-39.

nationale de la sécurité des systèmes d'information (ANSSI), who indicated that ENISA did not have the resources (either staff or budget) to play a role of cybersecurity crisis management and response, suggesting that the priority should be working at the member state level, instead.[199] Indeed, a proposal for a European Resolution was even introduced in the French Senate, questioning the grounds for the Cybersecurity Act, and arguing that it posed difficulties with the concept of subsidiarity.[200]

Objectively, ENISA's evolving governance structure appears to have worked rather well, as evidenced by the review of the Court of Auditors. The Court of Auditors issued a clean opinion on ENISA's accounts for 2018[201], with a reference to ENISA's internal audit report and an observation on a lack of sensitive post policy to identify sensitive functions and to define measures to mitigate the risk of vested interests[202], and 2017[203], with a criticism about the handing over process for an accounting officer (no hand-over report transmitted) and observations on the failure to post vacancies on the website of the European Personnel Selection Office and to conduct an analysis of the impact of Brexit upon its organisations, operations and accounts[204]. A clean opinion was issued for 2016, with comments that 'do not call the Court's opinion into question.' The Court concluded that core operational activities under Work Programme 2014 'have a clear connection to the legal mandate of ENISA' and that effectiveness was good. There was room to improve related to the division of ENISA between Athens and Heraklion offices, however. Its 2015 evaluation indicated that ENISA 'effectively meets its stakeholders' expectations' but that there was a need to improve

[199] Rolland, S., 2017. 'Cybersécurité: 'La question n'est plus de savoir si on va être attaqué,' *La Tribune Hebdomadaire*, 26 October 2017, p. 12.
[200] Sénat (France), 2017. N° 79, Proposition de résolution européenne au nom de la commission des affaires européennes, en application de l'article 73 octies du Règlement, portant avis motivé sur la conformité au principe de subsidiarité de la proposition de règlement relative à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relative à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) – COM(2017) 477 final, présentée par M. René Danesi et Mme Laurence Harribey, 9 November 2017, https://www.senat.fr/leg/ppr17-079.html.
[201] Court of Auditors, Annual reports on EU agencies for the financial year 2018, 24 September 2019, 2019 C 417/01, 11 December 2019, 3.11. European Union Agency for Network and Information Security (ENISA), at 76-77.
[202] *Id*., at 77. The Court of Auditors said ENISA should adopt a sensitive post policy 'without delay'.
[203] Court of Auditors, Annual reports on EU agencies for the financial year 2017, 18 September 2018, 2018/C 434/01, 30 November 2018, 3.11. European Union Agency for Network and Information Security (ENISA), at 79-80.
[204] *Id*., at 80.

communications with stakeholders.[205] A clean opinion was also issued for 2015,[206] as well as for 2014[207] and 2013[208], with only minor points raised, such as the late payment by the Greek authorities of the rent for ENISA's Athens offices[209]. In each instance, observations allowed for corrective actions and played a necessary role in good governance.

ENISA was created by a European Parliament and Council Act, which is also true under the EU Cybersecurity Act. Today, ENISA is without decision-making powers to adopt binding legal instruments, although it can adopt internal documents such as recommendations, guidelines, reports, work programmes and strategic plans. In principle, it has been the kind of agency to which accountability issues are less relevant.[210] Both Member States and the Commission are represented on ENISA's Management Board, although the Member States more so, and since the 2013 ENISA regulation, ENISA has an Executive Board, as well—a governing body described generally as 'a proper solution that accommodates both needs of large size and efficiency'.[211] One could argue, then, that at least prior to the EU Cybersecurity Act, provisions regarding ENISA's governance structures intended to ensure administrative accountability have been excessive. However, this view neglects the positive effect that governance has brought to the agency, and does not take into account the fact that such governance may have been rendered necessary, or at least desirable, as a result of the impact of the agency's creation of soft law measures.

8. ENISA AND ACCOUNTABILITY: ADDITIONAL COMMENTS

EU agencies are part of a growing executive power in Brussels that, when granted independence, may escape traditional controls and raise issues regarding accountability.[212]

---

[205] Court of Auditors, Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2016, together with the Agency's reply, 19 September 2017, 2017/C 417/25, 2017 OJ (C 417) 160, 161-162, 6 December 2017.
[206] Court of Auditors, Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015, together with the Agency's reply, 13 September 2016, 2016/C 449/25, 2016 OJ (C 449) 138,139, 1 December 2016.
[207] Court of Auditors, Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014, 8 September 2015, at 4.
[208] Court of Auditors, Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2013, 16 September 2014, at 5.
[209] *Id*., at 6.
[210] Busuioc, E.M., 2013, supra note 1, at 42-43.
[211] Vos, E., 2014, supra note 198, at 26.
[212] Busuioc, E.M., 2013, supra note 1, at 3-4.

'Task expansion' has resulted in agencies having regulatory (or semi-regulatory) functions, such as issuing guidelines for national application of EU law.[213] Two trends are noted regarding ENISA: first, additional provisions regarding accountability—especially administrative accountability—being added to its fundamental regulation. This is the case with the 2013 ENISA regulation, to which 2012 Common Approach[214] provisions have been added (some of which are mentioned above). This is also true of the EU Cybersecurity Act. Second, the tasks assigned to ENISA have increased, and with the EU Cybersecurity Act they increase greatly, although its powers still remain in the domain of soft law. As we have discussed, this latter fact would tend to indicate a greater need for accountability as ENISA evolves into a more important agency, in terms of missions, budget, size and power.

Moreover, agencies should be subject to supervision and control, with mandates constantly reviewed.[215] In the area of external relations, however, ENISA is an agency with a general mandate for international action, without explicit provision for Commission or Council supervision or control.[216] In the 2013 ENISA Regulation, a list of illustrations (these appear not to be limitative) of certain international action is added:

> (i) being engaged, where appropriate, as an observer and in the organisation of international exercises, and analysing and reporting on the outcome of such exercises;
>
> (ii) facilitating exchange of best practices of relevant organisations;
>
> (iii) providing the Union institutions with expertise.[217]

Nonetheless, the EU Cybersecurity Act introduces a requirement that Commission prior approval must be obtained for ENISA to establish working arrangements with international organisations and third country authorities; furthermore, such arrangements 'shall not create legal obligations incumbent on' the EU or Member States.[218] This may be seen as providing an ex ante control mechanism (as described by Busuioc), as ensuring that the Commission

---

[213] Egeberg, M., and Trondal, J., 2017. 'Researching European Union Agencies: What Have We Learnt (and Where Do We Go from Here)?', *Journal of Common Market Studies*, 55(4), 675-690.
[214] European Parliament, Council of the EU and European Commission, 2012. Joint Statement of the European Parliament, Council of the EU and the European Commission on decentralised agencies and Annex (Common Approach), 19 July 2012, https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.
[215] Vos, E., 2014, supra note 198, at 33.
[216] Ott, A., Vos, E. and Coman-Kund, F., 2014. 'European Agencies on the Global Scene: EU and International Law Perspectives' in *European Agencies in between Institutions and Member States* (M. Everson, C. Monda, & E. Vos, eds., Wolters Kluwer Law & Business), at 120. The authors refer to Regulation (EC) No 460/2004, art. 3.
[217] Regulation (EU) No 526/2013, supra note 135, art. 3(1)(f).
[218] Regulation (EU) No 2019/881, supra note 52, art. 42(1).

must act in order to allow such arrangements, and by setting out limitations through the law—adopted by the Council and the Parliament, and thus be considered part of the political accountability of the agency, as described by Vos (Section 2). Furthermore, this provision is consistent with what has been done with respect to other agencies, such as Europol and EASA.[219] In addition, the Commission is tasked with ensuring 'that ENISA operates within its mandate and the existing institutional framework by concluding appropriate working arrangements with the Executive Director.'[220] However, it should be pointed out that one reason for this participation of EU agencies internationally is 'the high degree of complexity which characterises external aspects of various policy areas of the Union' and where, given the 'very detailed and technical issues requiring a high level of expertise, the Council and the Commission may be inclined to allow the relevant specialised agency to play a role'[221] Arguably, this complexity could make monitoring and evaluating the work of any relevant agency in this regard as difficult, other than through box checking exercises regarding such agency's mandate, although Coman-Kund comments that most EU agencies pursue 'various forms of international cooperation'[222] and that ENISA has had a scarce (or scarcely-documented) international cooperation practice up to present[223].

While not a rule-making agency, ENISA is involved in identifying guidelines and best practices which are part of 'soft law' that allows data controllers to show compliance with security requirements under EU data protection law. If we look to the case of a rule-making agency developing 'soft law' contained in guidelines issued by another agency, the European Medicines Agency (EMA), these guidelines are non-legally binding but may be considered to have a 'quasi-binding character that can derive from the legal basis when the guideline intends to specify how to fulfil a legal obligation'[224]. While the situation of a non-rulemaking agency issuing guidelines is different, the point being made is that because of the importance of GDPR compliance and the fact that ENISA, the EU Cybersecurity Agency, has issued guidelines on this area of compliance, it could be argued that such 'soft law' likewise takes has a 'quasi-binding character', or, as Coman-Kund and Andone would say, an 'in-between' one, astride the boundary between legally-binding and non-legally-binding acts[225], which

[219] Vos, E., supra note 6, at 42.
[220] *Id*., art. 42(3).
[221] Coman-Kund, F., 2018, supra note 32, at 4.
[222] *Id*., at 53.
[223] *Id*., at 43.
[224] Chiti, E., 2013, supra note 187, at 98.
[225] Coman-Kund, F. and Andone, C., 2019, supra note 69, at 178.

would seem to argue for greater political accountability. Furthermore, certain academic legal theories posit that through coercive enforcement, soft law may become hard law, through judicial intervention, for example[226]. However, any such enforcement would involve an indirect path between ENISA and, say, data protection authorities, or the Commission, prior to such enforcement. That is, data protection authorities could use soft law created by ENISA in order to find that a data controller had not met security requirements or privacy by design requirements under the GDPR. While there are Member State cybersecurity agencies and standardisation bodies that also issue cybersecurity guidelines, which the data protection authorities could look to, it seems that from the perspective of legal certainty related to rule of law concerns, data controllers and processors should be able to rely on ENISA soft law instruments in order to prove their compliance with provisions of the GDPR, although in another field—competition law—discretion of Member State authorities has prevailed over individual expectations, and this has led one academic to comment that 'courts do not really enforce soft law, but the legal principles and values soft law is expected to foster'[227]. Moreover, when ENISA proposes candidate certification schemes under the Cybersecurity Act, a pre-law function, these have to be adopted by the Commission under an implementing act. Thus, there is a decision-maker between ENISA and the enforcement and law-making, which may be looked to for political accountability and whose decisions may be judicially reviewed.

Nonetheless, Rocca and Eliantonio argue that, as there is a general lack of ex post control with respect to agency soft law, there should be some form of ex ante control, and that 'the procedure that leads to the adoption of soft law becomes an important factor to establish the legitimacy of agencies' soft law-making'[228]. Arriving at such legitimacy involves transparency, which also is a concern discussed in the context of ex post accountability, although here the focus is on transparency specifically in the law-making that is of concern—allowing access to the soft-law documents, knowledge of 'who is accountable for the final document and who has to be consulted in the process'[229]. Rocca and Eliantonio divide agencies into four groups, based on the kinds of soft law they issue: (1) soft law measures that contain technical and specific guidelines, which explain requirements for compliance with specific EU law (as an example, EASA is placed in this group); (2) soft law measures that

[226] Ștefan, O., 2017, supra note 66, at 211.
[227] *Id*., at 210-211.
[228] Rocca, P. and Eliantonio, M., 2019, supra note 11, at 6.
[229] *Id*., at 10.

come in the form of technical guidelines, mainly helping explain the process for applications for sector-specific authorisations (EMA is an example); (3) soft law aimed at disseminating comprehensible and high-quality information; and (4) soft law 'in the form of technical documents mainly addressed to the Commission in order to help it develop further EU legislation', such as recommendations on possible amendments to current legislation in the information security sector by ENISA, which they put in this category.[230]

This simplification ignores the multi-faceted role of work by agencies such as ENISA, whose work product in the area of cybersecurity and privacy by design may be considered to explain requirements for compliance with the data protection legislation—the GDPR—thus falling within the first category, and whose role is also to disseminate high-quality information—consistent with the third category. Although the claim is that ENISA should be expected to have a medium level of legitimacy[231], as the soft law is internal in that it is addressed to the Commission, it may be more appropriate to have a high level of legitimacy for its work that fits into the first category, instead. In that category there is a higher level of proceduralisation, with detailed rules as to public access to documents, and indicating who is accountable for the soft law issued, and separate rules of procedure explaining which stakeholders must be consulted in the decision-making process.[232] The real difference between EASA, in the first category, and ENISA, which has been placed by Rocca and Eliantonio in the fourth, is what they describe as 'participation'. In this category, EASA is described as having 'Separate detailed rules of procedure on how to adopt soft law (including the stakeholders to be consulted)'[233] and ENISA as having only 'General articles in the Regulation about the transparency of the agencies' procedures'[234], instead. This argues in favour of the implementation by ENISA of greater procedural rules on the adoption of soft law measures, as ex ante controls.

Moreover, the development of ENISA has been described (before the EU Cybersecurity Act) as part of an 'institution-building strategy that was adopted in the early 2000s'[235]. In its initial years, 'some cyber security policy issues were moved away from the EU institutions,

[230] *Id*., at 12-13.
[231] In fact, in testing their hypotheses, the authors determine that ENISA has a low level of legitimacy, instead. *Id*., at 28.
[232] *Id*., at 15.
[233] *Id*., at 20.
[234] *Id*., at 27.
[235] Ruohonen, J., Hyrynsalmi, S., and Leppänen, V., 2016. 'An outlook on the institution evolution of the European Union cyber security apparatus', *Government Information Quarterly*, 33, 746-756, at 750.

including the European Parliament, the [Commission], and the Council, to bureaucratic institutions such as ENISA'[236], a non-elected body, which raises questions of political accountability, as well. Furthermore, ENISA acts in a highly technical area, where 'Member States and EU bodies rely on its substantial expertise on cybersecurity matters.'[237] While greater expertise could be built up in the EU institutions, so that they best be able to control the work of ENISA, this would negate the value of efficiency of an agency, and perhaps its independence as well.

Members of one of ENISA's governance structures, its Advisory Group, only have a right to attend Management Board meetings when invited, contrary to the non-voting stakeholder members of the Management Board, prior to ENISA's 2013 governance structure reforms. Indeed, at that time the former stakeholder representatives on the Management Board who were thus not re-appointed, became members of the Permanent Stakeholders' Group, instead.[238] Thus, experts from stakeholders are not automatically included at meetings of the Management Board where important operational decisions are made. This may be seen as a weakness, given ENISA's role and the importance of the advisers' advice and connection to stakeholders. Although these advisers include five members from academia, certain commentators have criticized ENISA saying that it 'seems to intentionally distance itself particularly from academic research'[239].

In addition, '[t]here is no other actor at EU level that supports such broad scope of network and information security stakeholders.'[240] The European Parliament committee with responsibility for ENISA is the Industry, Research, and Energy Committee (ITRE).[241] However, there are many demands on MEPs time, and high MEP turnover, which might limit the time that specific MEPs may have to build up the technical expertise necessary for properly providing administrative oversight in this area.[242] The result is that there may be the development of an oversight problem related to the fact that the agency is more expert on

[236] *Id*. at 754 (citation omitted).
[237] European Commission, 2017b, supra note 180, at 15.
[238] ENISA, Decision No. MB/2014/7 of the Management Board of the European Union Agency for Network and Information Security on the Establishment and Operation of the Permanent Stakeholders' Group, 28 October 2014, https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions/mb-decision-no-mb-2014-7-on-internal-rules-of-operation-of-psg.
[239] Ruohonen, J., Hyrynsalmi, S., and Leppänen, V., 2016, supra note 256, at 752.
[240] *Id*. at 6.
[241] Jacobs, F., 2014. 'EU Agencies and the European Parliament' in *European Agencies in between Institutions and Member States* (M. Everson, C. Monda, & E. Vos, eds., Wolters Kluwer Law & Business), at 213.
[242] *Id*., at 227.

cybersecurity issues than the legislature,[243] indicating a concern for political accountability. This will become truer if ENISA obtains greater powers and is an area that merits further study.

Insofar as what Vos calls financial accountability is concerned, the Parliament plays a role through the discharge procedure.[244] It 'allows for a 'written dialogue' between the Committee on Budgetary Control and the relevant agency', often based on observations of the Court of Auditors, but it may also include issues from the agency's annual activity report or other issues the Parliament considers relevant[245], thus extending to ongoing control of the agency and limiting its autonomy. There is also a verbal exchange between the committee and the agency, when considered necessary.[246] If one discharge of ENISA is taken as an example, it may be noted that there is extensive discussion of the agency's budget and staffing, of the agency's future whistleblowing policy, of transparency (for example, the lack of CVs and declaration of interest of the Management Board Members, and of the need for a 'proactive lobby transparency policy'), that Council makes a recommendation on discharge, but there is no mention of any soft law measures which might have been included in ENISA's activity report.[247]

9. Concluding Remarks

Information-providing agencies such as ENISA seem less problematic insofar as accountability is concerned, and we have seen that changes in ENISA's fundamental regulation have brought it into line with the Common Approach on EU Agencies, providing elements of accountability and control to an agency that has stood out because of its time limited mandate. However, we have also seen that, given ENISA role as a maker of soft-law, this one-size-fits all approach may not be suitable, especially insofar as what Rocca and Eliantonio call participation. The provisions implemented in order to ensure administrative accountability of ENISA may be seen by some to have been excessive, given the limited

[243] Busuioc, E.M., 2013, supra note 1, at 59.
[244] Vos, E., 2018, supra note 6, at 9 ('financial accountability which concerns the role of the Commission's financial controller, the Council and the European Parliament as budgetary authorities, the latter of which is also responsible for the annual budgetary discharge and the Court of Auditors').
[245] Busuioc, E.M., 2013, supra note 1, at 180.
[246] *Id*., at 181.
[247] Decision (EU) 2017/1690 of the European Parliament of 27 April 2017 on discharge in respect of the implementation of the budget of the European Union Agency for Network and Information Security for the financial year 2015, 2017 OJ L 252/267, 29 September 2017, and the attached Resolution (EU) 2017/1691 of the European Parliament of 27 April 2017 with observations forming an integral part of the decision on discharge in respect of the implementation of the budget of the European Union Agency for Network and Information Security for the financial year 2015, 2017 OJ L 252/268, 29 September 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2017:252:FULL&from=EN.

mission and small budget and staff of the agency, although it has been shown that checks, such as observations of the Court of Auditors, have provided grounds for improvement in ENISA's case. The recently adopted EU Cybersecurity Act increases ENISA's powers, and we have seen that the role that that agency plays in EU legislation in the fields of data protection, electronic privacy and cybersecurity, particularly through the creation of soft law, give it a stronger role than might otherwise be expected, although still in the realm of a contributor to policy, and a maker of soft law. This places it squarely within what Coman-Kund has described as agencies' being 'placed 'at a crossroads' between implementation and decision-making, between expertise and policy-making, in a complex environment populated with various actors from different levels of governance.[248] Part of the solution may be to implement ex ante control in the form of a greater procedurisation of law-making, as discussed by Rocca and Eliantonio. Finally, the oversight problem that might exist with respect to ENISA's cybersecurity expertise warrants further study and consideration in the context of accountability.

As a final thought, the area of cybersecurity is one where there is greater and greater need for centralised action and standards. Although cybersecurity has been argued to be almost exclusively the ambit of Member States, the EU has claimed nevertheless that it is 'too complex and too transnational in nature to be left to Member States'[249]. Consistent with this thought, and with the ongoing general trend to supranationalism of EU executive power noted by Vos (amongst others)[250] this may be the natural tendency for cybersecurity, too. Historical divisions between the original pillars act as a brake to this today. If at some future point the Member States could be convinced of the desirability of handling (and not merely coordinating or facilitating) cybersecurity at the EU level, ENISA might see its mission greatly increased, at which time the question of accountability for the agency, especially related to the 'expertification of decision-making'[251], would become all the more important.

[248] Coman-Kund, F., 2018, supra note 32, at 53.
[249] Carrapico, H. & Barrinha, A., 2017, supra note 38, at 1266.
[250] Vos, E., 2018, supra note 6, at 18-19.
[251] Eriksen, A., 2019, supra note 196, at 1 (referring to Vibert's term 'rise of the unelected').