Cybersecurity is Gaining Momentum – NIS 2.0 is on its Way

*Sandra Schmitz-Berndt**

I. Introduction

The security of network and information systems is an important part of data protection, in particular when data processing is carried out through the use of information and communication technologies.[1] In parallel to the entry into force of the GDPR in May 2018, the first piece of EU-wide cybersecurity legislation, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ('NIS 1.0')[2], had to be transposed into national law by May 2018.

Undoubtedly, the NIS Directive contributed to a significant change in the regulatory approach to cybersecurity in many Member States. However, increased digitisation of the internal market and digital transformation of society as such means that the threat landscape concerning attacks against digital infrastructure and solutions evolves and new challenges emerge. The first periodic review of the NIS 1.0, initially foreseen for completion in May 2021, accelerated – especially concerning the conclusions to be drawn – with the COVID-19 crisis and resulted in a proposal by the European Commission for a revised NIS Directive ('NIS 2.0')[3] as early as December 2020. Very recently, on 28 October 2021, the European Parliament's Committee on Industry, Research and Energy (ITRE) adopted its report on the NIS 2.0 Proposal[4], suggesting various amendments to the Commission's proposal.[5]

This contribution highlights how the proposed NIS 2.0 addresses shortcomings identified in the current version of the NIS Directive and comments on the amendments suggested by ITRE.

II. NIS 1.0: Shortcomings and Deficits

The review process of the NIS 1.0 identified limitations as well as deficiencies that presumably prevented the NIS Directive from 'unlocking its full potential'[6].

First of all, a weakness of NIS 1.0 is its limited scope of application, since the Directive only applies to providers of certain digital services and operators of essential services restricted to the sectors energy, transport, banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure.[7] Due to this limitation, the NIS 1.0 fails to address the increased interconnectedness and interdependencies in sectors not covered.[8] This may result in companies not sufficiently investing in cybersecurity because they are outside the scope of the Directive; nevertheless protection of these companies may be of similar importance.[9]

DOI: 10.21552/edpl/2021/4/14

* Sandra Schmitz-Berndt is Research Associate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) at the University of Luxembourg. For correspondence <sandra.schmitz@uni.lu> The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, <https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/>.

1 EDPS, Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA) (20 December 2010) <https://edps.europa.eu/sites/default/files/publication/10-12-20_enisa_en.pdf> accessed 30 November 2021.

2 [2016] OJ L 194/1.

3 European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

4 European Commission, ITRE, Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)), A9-0313/2021 (4 November 2021) https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.pdf> accessed 30 November 2021.

5 The report was adopted with 70 votes in favour, 3 against and 1 abstention.

6 (n 3), Explanatory Memorandum.

7 See Annex II NIS 1.0.

8 European Commission, Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – No. 2020-665, Final Study Report (January 2021), 80.

9 Cf. ibid, 82

The Final Report of the Study to support the review of the NIS 1.0 concluded that too broad discretion is given to the Member States in defining the de facto scope of the Directive.[10] A major point of criticism has also been the vagueness of provisions and resulting unclear requirements[11] which in sum with the divergence across Member States in the implementation of the Directive resulted in a fragmented regulatory policy landscape. Member States are for instance supposed to define and identify operators of essential services in the sectors encompassed by the NS 1.0 in their territory by themselves. NIS 1.0 does not provide guidance as to how the identification process should be carried out. This minimum harmonisation approach resulted in national identification methodologies that differ significantly in terms of which types of services national authorities deem to be an essential service.[12] Significant inconsistencies also exist in the way the national thresholds are applied.[13] Preliminary evidence from the review process also suggests that the divergence between Member States may be related to two factors: the delegation of the identification process to sectoral authorities (e.g. ministries, agencies) and the top-down versus bottom-up (self-identification) identification procedure.[14] As a consequence, there is no consistent treatment of entities in the sectors covered by the Directive across the Member States.

Despite the discrepancies in the selection and definition of critical sectors and essential services, the information sharing about incidents and vulnerabilities is still limited. Cooperation is however a central element of the NIS 1.0, which aimed to increase EU-level cooperation through the creation of two new fora: the NIS Cooperation Group[15] (to support and facilitate the strategic cooperation and exchange of information among Member States) and a network of Computer Incident Response Teams[16] (CSIRTs) (to improve the handling of cross-border incidents, share information about risks and coordinate responses to specific incidents). Further, Member States are required to designate a national central contact point as liaison office for supranational cooperation.[17] In practice, collaboration between the Cooperation Group and CSIRTs network turned out to be insufficient.[18] Operational information sharing focused on cross-border incidents, whereas the need to share information on vulnerabilities across Member States to ensure more robust risk management is hardly addressed.[19]

In order to increase the cyber resilience of operators of essential services and digital service providers covered by the Directive, the NIS 1.0 foresees the implementation of security measures (following a risk-based approach) and introduces an obligation to report incidents.[20] As with the identification procedure, the transposition of the respective articles varies significantly.[21] With no need to ensure coherence with certification schemes as stipulated by the Cybersecurity Act[22], there are Member States with detailed legislation on security measures, while others provide no guidance at all.[23] The obligations imposed upon operators of essential services and digital service providers are similar yet not identical.[24]

Different approaches in the transposition and in some cases pre-existing legislation[25], are one reason why security measures and incident reporting requirements are inconsistent across Member States.

10 Ibid, 80.

11 Ibid.

12 European Commission, Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM/2019/546 final.

13 Ibid.

14 (n 8),84 et seq.

15 The NIS Cooperation Group was established by Article 11 NIS 1.0 with the aim to ensure strategic cooperation and the exchange of information in cybersecurity among EU Member States.

16 See Article 12 NIS 1.0. The national CSIRTs collaborate in the CSIRTs Network 'to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation'.

17 Art. 8(3) NIS 1.0.

18 (n 8), 82.

19 Ibid, 83.

20 Cf. Arts. 14 and 16 NIS 1.0.

21 (n 8), 85 et seq.

22 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15.

23 Cf. (n 8),83. No legislation has for instance been passed in Luxembourg.

24 Cf. Arts. 14 and 16 NIS 1.0.

25 Such as for instance the German IT security Act, the Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), which has only recently been extended by the IT-Sicherheitsgesetz 2.0 (IT Security Act 2.0).

Another reason is that there is no common set of criteria as to what is considered an appropriate security measure in view of the risk posed and what is considered an incident.[26] For instance, in 2018 the Hungarian authority received only 900 incident reports, while the Lithuanian authorities received 10.000.[27]

Uncertainties for reporting entities also arise from the fragmented supervisory landscape in some Member States[28]: while almost half of the Member States employ a centralised approach with one NIS supervisory authority,[29] other Member States opted for a decentralised approach with sector-specific regulatory bodies[30]. The fragmented supervisory landscape has been deemed to create uncertainty in terms of accountability and responsibility to supervise incident notification.[31]Also, the review process identified different approaches to enforcement, inter alia in terms of regime of sanctions and penalties.[32] In fact, the penalties applicable to infringements of national provisions implementing the NIS 1.0 vary significantly.[33]

Finally, Article 7NIS 1.0 required Member States to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of cybersecurity.

Besides the magnitude of obligations imposed on Member States, an impact assessment in 2020 identified inter alia a low level of cyber resilience of businesses operating in the EU as well as inconsistent resilience across Member States and sectors.[34]

III. The Commission's Proposal for a NIS 2.0 Directive: Making Europe Fit for the Digital Age

Despite the deficiencies outlined in the examples above, the Commission acknowledges an improvement of the overall level of cybersecurity at national level and an increased cooperation between Member States to exchange strategic and operational information. However, recognising that the NIS 1.0 paved the way for a change in mind-set in relation to the institutional and regulatory approach to cybersecurity in many Member States, the Commission concludes that this development has reached its limits.[35] Thus, on 16 December 2020, the European Commission adopted the aforementioned Proposal for a NIS 2.0 Directive. The proposal is part of a package of measures to further improve the resilience and incident response capacities of public and private entities, competent authorities, and the Union as a whole in the field of cybersecurity and critical infrastructure protection. The package also includes a new Strategy on Cybersecurity[36] and a Proposal for a Directive on the resilience of critical operators of essential services[37], which aims to mitigate physical threats against such operators.

A key change of the Commission's NIS 2.0 Proposal relates to the scope of the Directive: new sectors are added including waste water, public administration and space; several existing sectors are amended.[38] The NIS 2.0 Proposal further expands cooperation between the national competent authorities to exchange information, while also expanding the tasks of the existing NIS Cooperation Group and the CSIRT network.[39] In addition to the two established cooperation networks, the proposal foresees the integration of a further network to deal with large-scale incidents that impact multiple Member States under its umbrella: The European cyber crises liaison organisation network (EU-CyCLONe).[40] This network was launched in 2020 and aims to contribute to the implementation of the European Commission Blueprint for rapid emergency response in case of a large-

26 (n 8),88.

27 Ibid.

28 NIS 1.0 required Member States to designate competent authorities in the field of network and information security for inter alia monitoring compliance.

29 For instance, Austria, Belgium, France, and Germany.

30 For instance, Czechia, Luxembourg, the Netherlands, and Poland.

31 (n 8),88.

32 Ibid, 89.

33 Ibid, 55 et seq. Variations even exist at Member State level depending for instance on the sector concerned.

34 European Commission, Commission Staff Working Document, Impact Assessment Report, Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, SWD(2020) 345 final.

35 (n 3), Explanatory Memorandum.

36 European Commission, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final.

37 European Commission, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, COM/2020/829 final.

38 See (n 3), Annexes I and II.

39 Ibid, Arts. 12 and 13.

40 Ibid, Art. 14.

scale cross-border cyber incident or crisis.[41] It complements the pre-existing cooperation networks by linking the cooperation at technical level (CSIRTs network) and policy level (NIS Cooperation Group).

The proposal also introduces a framework for coordinated vulnerability disclosure with designated CSIRTs as trusted intermediaries to facilitate the interaction between the reporting entity and the manufacturers or providers of ICT products and services. Responding to the lack of information exchange regarding vulnerabilities, the NIS 2.0 Proposal tasks ENISA to develop and maintain a European vulnerability registry for discovered vulnerabilities.[42]

As regards the structure of the NIS 1.0, the proposal eliminates the distinction between operators of essential services and digital service providers. Rather than distinguishing between the type of service provided, the proposal introduces a classification based on the importance of the service provided. The NIS 2.0 Proposal distinguishes between 'essential entities' (see Annex I) and 'important entities' (see Annex II). Whether a service provider falls within the scope of the Directive is determined by a single criterion applied across all Member States, namely the entity's size. By this stand-alone criterion, the Commission responds to the fragmentation across the EU under the NIS 1.0. According to Article 2(1) NIS 2.0 Proposal, an entity is within the scope of the Directive if it belongs to one of the economic sectors listed in Annexes I and II and is not considered a micro or small enterprise.[43] There are, however, a few exceptions to the size-cap rule.[44]

Following the risk-based approach adopted by the NIS 1.0, the NIS 2.0 Proposal enlists basic security elements. Of the catalogue of measures that entities have to observe, a new measure that needs to be mentioned is the supply chain security. The divergences in incident reporting shall be eliminated by more precise provisions, i.e. a tiered plan, on the incident reporting process.[45] Besides the reporting of incidents that have caused or have the potential to cause harm, reportable incidents also encompass significant cyber threats in order to get a full picture of the threat landscape. It has to be noted that by way of deletion in sector-specific acts, the security requirements and notification obligations relating to cybersecurity incidents, are now mainly united under the NIS 2.0 umbrella. This eliminates any issues as to whether a sector-specific act provides measures with equivalent effect and can therefore be deemed lex specialis under Art. 1 (7) NIS 1.0. A further new aspect in the NIS 2.0 Proposal is the responsibility and accountability of management bodies and their members for the compliance with cybersecurity requirements. In light of corresponding notification obligations – also in relation to personal data breaches – that remain in other EU legal interventions,[46] the proposal encourages Member States to establish a single entry point for all notifications 'required under this Directive and also under other Union law such as Regulation (EU) 2016/679 and Directive 2002/58/EC'.[47]

Finally, supervision of the entities encompassed is split into an ex ante supervisory regime for essential entities and a lighter, ex post, supervisory regime for important entities.

IV. The ITRE Draft Report: Making Europe even Fitter for the Digital Age?

In May 2021, the European Parliament's Committee on Industry, Research and Energy published a draft report on the Commission Proposal for a NIS 2.0 Directive ('Draft Report')[48] suggesting several amendments[49].

The Rapporteur welcomes the expansion of the scope of the Directive proposed by the Commission,

41 ENISA, Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe)(29 September 2020) < https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone> accessed 30 November 2021.

42 (n 3), Art. 6.

43 See the definition in Art. 2(2) in Annex to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36.

44 Cf. (n 3), Art. 2(2).

45 Cf. ibid, Art. 20(4).

46 For an overview of EU incident reporting schemes seeS Schmitz-Berndt and F Anheier, 'Synergies in Cybersecurity Incident Reporting – The NIS Cooperation Group Publication 04/20 in Context' [2021] EDPL 101.

47 (n 3), Recital 56.

48 European Commission, ITRE, Draft Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)) (3 May 2021); Rapporteur: Bart Groothuis.

49 In total the Rapporteur suggests 91 amendments.

and suggests a further sector to be included, namely research and academic institutions[50], arguing that they are on the one hand, heavily targeted and on the other hand, intellectual property deserves equivalent protection from outside attacks.[51]

Key changes to the Commission's proposal relate to the reportable incident and the notification procedure. In recognition of the importance of incident reporting to increase the security of NIS, the Rapporteur criticises the timeframe within which an initial report has to be filed and suggests an alignment with the GDPR, under which personal data breaches have to be reported within 72 hours.[52]

The argument of alignment with further EU interventions[53] can easily be rebutted if one consults other interventions such as the Proposal for a Regulation on digital operational resilience for the financial sector ('DORA')[54]: reporting of security incidents in the financial sector requires much shorter timeframes (Art. 17 DORA Proposal[55]). Also, by increasing the timeframe to 72 hours, reporting may become of secondary interest. Considering the very basic information required in the initial report as foreseen in the Proposal, this is unlikely to be overly burdensome at this stage.

The report is very critical on extending the scope of a reportable incident. First of all, the requirement to report incidents that only have the potential to cause harm or affect others is considered as unrealistic.[56] There is fear that the competent national authorities could be overwhelmed by receiving too many notifications, which in turn could divert attention and limit security resources away from the essential tasks of actually examining and handling incidents.[57] Further, entities may find it impossible to know if a cyber threat 'could have potentially resulted in a significant incident'.[58] In addition, it is argued that a cyber threat and a report-worthy cyber incident are not the same thing.[59] Accordingly the Draft Report suggests to delete the reporting obligation as regards cyber threats and such incidents that have the potential to cause harm from the Proposal.[60] While over-reporting cannot be excluded, no evidence is presented that the requirement to report 'incidents that did not cause harm' challenges the handling of actual incidents. For instance, the German implementation of the NIS 1.0 foresees such reporting[61], but there are no reports as to whether this has resulted in the feared over-reporting. In fact, the German national NIS authority only received 419 incident reports in total from June 2019 to Mai 2020.[62] Considering that a near miss may be the result of appropriate cybersecurity, reporting complements the evaluation of the overall threat landscape. Such an incident affecting a service provider may still constitute a severe threat to other service providers. However, if incidents that only have the potential to cause harm and cyber threats[63] are to be included as reportable, then it must at least be clearly defined what constitutes a cyber threat for example, or whether this should already be an email which is easily to be identified as phishing attempt.

As regards the mandatory reporting of potential cyber threats, the Rapporteur also argues that compliance and liability will discourage the activities of threat hunters.[64]

Concerns are also raised about the scope of application being potentially too broad, bearing the risk that users who employ their own DNS service fall under the scope of the Directive.[65] Similar concerns are raised regarding the inclusion of operators of root

50 (n 48), Amendment 91.

51 Ibid, 56.

52 Ibid, Amendment 61.

53 Ibid, 57.

54 European Commission, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM 2020/595 final.

55 According to Art. 17(3) DORA Proposal, financial entities must submit an initial notification without delay, but no later than the end of the business day, or, in case of a major ICT-related incident, no later than four hours from the beginning of the next business day if the incident occurred later than two hours before the end of the business day.

56 (n 48), 57.

57 Ibid.

58 Ibid, Amendment 57.

59 Ibid.

60 Ibid.

61 § 8b (4) no 2 BSI-Gesetz.

62 Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2020* (September 2020), 54 <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1> accessed 30 November 2021.

63 Art. 4(7) refers as regards the definition of cyber threat to Art. 2(8) of Regulation (EU) 2019/881, which defines a cyber threat as meaning 'any potential circumstance, event or action that could damage, disrupt or otherwise adverserly impact network and information systems, the users of such systems and other persons'.

64 (n 48), 57

65 Ibid.

name servers in the scope of the Directive; in that perspective, regulation of these services is not desirable since root name servers are operated by expert-volunteers, who do not monetise their service.[66] Accordingly, the rapporteur suggests to replace the wording in recital 15 of the Proposal clarifying that these kind of operators shall not be included.[67]

Although the Commission's Proposal contains a clear commitment to extend information sharing, the rapporteur does not agree on the result. In fact, in his opinion, information sharing will be severely hampered and should also include information sharing with partners outside the EU.[68] This conclusion, however, needs further explanation.

The Report also suggests to replace the proposed European vulnerability registry with a vulnerability database leveraging the global Common Vulnerabilities and Exposures (CVE) registry.[69]

In line with new tasks for the CSIRTs such as inter alia the role of trusted intermediary in coordinated vulnerability disclosure, the report emphasises the Member States' need to prepare CSIRTs for the extended tasks and improve the technical capabilities of the teams.[70]

Finally and very importantly, the Parliament, in its Draft Report, also addresses the relationship of the NIS Directive to Union legislation on personal data protection. While the Commission's Proposal, beside clarification that it is without prejudice to the GDPR and ePrivacy Directive, remains silent about personal data processing, the suggested amendments introduce more precise references to the GDPR and legitimate data processing.[71]

V. Current Status of the NIS 2.0 Proposal

The Draft Report of May 2021 as outlined above saw editorial and further minor amendments before its adoption within the ITRE committee.[72] Those amendments inter alia relate to the reporting timeframe which has been reverted to 24 hours, but only with regard to incidents that significantly disrupt the availability of the service concerned.[73] In accordance with the Draft Report, no obligation exists to report incidents that have the potential to cause harm and cyber threats; Instead the recipients of the service affected should be informed of protective measures or remedies to such known risks.[74] An emphasis is further put on the adoption of a national cybersecurity strategy that goes beyond the initial Commission's Proposal.[75] Following the adoption of the Report within the Committee and the first reading, the Proposal is now subject to negotiations between the co-legislators. The Council has already raised a number of concerns inter alia in relation to the interaction with sectoral legislation and the significant expansion of scope.[76] The trilogue is thus eagerly awaited. Considering the speed of the initial review of the NIS 1.0 and the challenges posed by the COVID-19 crisis it is unlikely that the time it takes to adopt a NIS 2.0 will reach the three years it took to adopt NIS 1.0.

66 Ibid.

67 Ibid, Amendment 1.

68 Ibid, 58.

69 Ibid, Amendment 6.

70 See for instance ibid, Amendments 40 et seq.

71 Cf. for instance ibid, Amendment 23, Amendment 68, Amendment 90.

72 (n 4).

73 Ibid, Amendment 204.

74 Ibid, Amendment 195.

75 See European Commission, *A high common level of cybersecurity, Committee Report tabled for plenary, 1st reading/single reading, 2020/0359(COD)* (04.11.2021) <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1681091&t=e&l=en> accessed 30 November 2021.

76 Council of the European Union, TTE Council, *Background Press release* (31.05.2021), 3 <https://www.consilium.europa.eu/media/50000/background-brief-telecoms_en-june-2021.pdf> accessed 30 November 2021.