THE UPCOMING NETWORK CODE ON CYBERSECURITY AND ITS IMPACT ON RESILIENCE OF THE EUROPEAN ENERGY SECTOR

František Kasl / Lucie Chmelíčková / Martin Švec

František Kasl, Ph.D., postdoctoral researcher, Masaryk University, Faculty of Informatics, Centre for Education, Research and Innovation in Information and Communication Technologies, Botanická 554/68a, 602 00 Brno, CZ, e-mail: frantisek.kasl@muni.cz

Lucie Chmelíčková, researcher, Masaryk University, Faculty of Informatics, Centre for Education, Research and Innovation in Information and Communication Technologies, Botanická 554/68a, 602 00 Brno, CZ, e-mail: 434380@muni.cz

Martin Švec, Ph.D., postdoctoral researcher, Masaryk University, Faculty of Informatics, Centre for Education, Research and Innovation in Information and Communication Technologies, Botanická 554/68a, 602 00 Brno, CZ, e-mail: 325544@muni.cz

Keywords: ***network code on cybersecurity, energy sector, cybersecurity, smart grid, European law***

Abstract: *The cybersecurity challenges in the European energy sector have significant cross-border element that needs to be reflected in the collaboration and coordination on obligations and rules applicable to the system operators. The rules for transmission system operators are developed by European Network of Transmission System Operators for Electricity (ENTSO-E). In early 2024, new transformative rule book for cross-border cybersecurity will be established through the upcoming Network Code on Cybersecurity (NCCS). In our contribution, we introduce the NCCS, procedure leading to its adoption, core concepts, main provision and likely impact. Subsequently, we discuss in detail its expected benefits and weaknesses as well as suitable future progress in line with the development of robust and resilient European energy infrastructure with regard to cybersecurity.*

1. Introduction[1]

Against the backdrop of a rapid digitalisation of various sectors, including the energy sector, cybersecurity challenges appear to be even more pressing. It is worth noting that digitalisation is viewed as a key enabler of the energy transition accelerating both integration of more renewable energy and decarbonisation of the sector. The European Union has implemented several legal frameworks to improve cybersecurity across sectors and industries. Recently adopted frameworks are based on the Security Union Strategy[2] and the EU's Cybersecurity Strategy for the Digital Decade.[3] They aim to ensure a high common level of cybersecurity in all EU Member States, boost the overall level of cybersecurity, and improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The methodology adopted in this paper employs a doctrinal analysis to explore relevant policy context leading to the adoption of the Network Code on Cybersecurity. Additionally, it conducts an examination of the existing legal framework and its prospective interaction or compatibility with the Network Code on Cybersecurity. Given the pending adoption of the network code, the authors direct their primary attention toward exploring its developmental phase and analysing the diverse roles enacted by stakeholders influencing the eventual

[1] This article is based upon the grant of the Technology Agency of the Czech Republic, THETA programme, Decentralized Control of Distribution System (DECODIS) – TK04020195.

[2] Cf. European Commission, Communication from the Commission on the EU Security Union Strategy COM(2020) 605 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (accessed on 18 December 2023), 2020.

[3] Cf. European Commission, The EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 final. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 (accessed on 18 December 2023), 2020.

shaping of its final wording. Subsequently, the authors scrutinize the latest available version of the network code.

2. Related EU level legal framework

The EU has a systemic approach to address cybersecurity related threats combining the cross-sector cybersecurity frameworks (established by the NIS 2 Directive or the Critical Entities Resilience Directive (CER)), and sector-specific measures (such as the Regulation on risk-preparedness in the electricity sector (EU) 2019/941). The most relevant cross-sector cybersecurity related frameworks adopted or proposed at the EU level include:

- **The NIS2 Directive**:[4] The NIS2 Directive is the EU-wide legislation on cybersecurity that aims to provide legal measures to improve the overall level of cybersecurity in the EU mainly by means of unification and it various different sectors such as digital services, health, transportation etc. It modernized the existing legal framework established by the NIS Directive to keep up with increased digitization and an evolving cybersecurity threat landscape.
- **The Critical Entities Resilience Directive (CER):**[5] The CER aims to enhance protection and resilience of entities providing services essential for the maintenance of vital societal functions or economic activities including the energy sectors. The directive explicitly states that it shall not apply to matters covered by the NIS2 Directive. Due to the relationship between the physical security and cybersecurity of critical entities, CER and NIS2 should be implemented in a coordinated manner.
- **Cyber Resilience Act (CRA):**[6] A proposed regulation on cybersecurity requirements for products with digital elements. The CRA aims to establish common cybersecurity standards for digital products and connected services sold in the EU market, protecting consumers and businesses from cyber incidents. The Act seeks to introduce mandatory cybersecurity requirements for manufacturers and retailers of products with a digital component. On 30 November 2023, a provisional agreement on the CRA was reached https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/.[7]

The NIS2 Directive defines the energy sector as one of the EU's critical infrastructures and provides for cybersecurity obligations related to supply chain security and risk-management measures. While the NIS2 Directive aims to prevent fragmentation of cybersecurity provisions across EU legal acts, in cases where additional sector-specific acts related to cybersecurity risk management measures and reporting obligations are deemed necessary, and the implementation of further provisions under the NIS2 Directive is not considered suitable due to the specificities and complexities of the concerned sectors, the NIS2 Directive does not prohibit the adoption of additional sector-specific Union legal acts addressing cybersecurity risk management measures and reporting obligations.

It is worth noting that EU Security Union Strategy acknowledges the need for sector specific initiatives making critical infrastructure more resilient against physical, cyber and hybrid threats. This includes the energy sector. Strengthening cybersecurity and resilience in the energy systems is one of the pillars of an EU action

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555 (accessed on 18 December 2023).

[5] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 18 December 2023).

[6] Proposal for a Regulation (EU) on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 (accessed on 18 December 2023).

[7] Cf. Council of the EU, Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products. https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/ (accessed on 18 December 2023), 2023.

plan - Digitalising the energy system[8] adopted in 2022, since cybersecurity is viewed as an essential requirement for the reliability of the increasingly digitalised energy system.

The most relevant energy sector specific act addressing cybersecurity so far adopted at the EU level is the Regulation on risk-preparedness in the electricity sector (EU) 2019/941, which complemented the NIS Directive by ensuring that cybersecurity incidents in the electricity sector are properly identified as a risk and that the measures taken to address them are properly reflected in the risk-preparedness plans. Further detailed cybersecurity related acts may be adopted by the European Commission as delegated acts. More specifically, Article 59(2)(e) of Regulation (EU) 2019/943 empowers the Commission to adopt delegated acts, so called "network codes", on sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

3. Safeguarding cybersecurity in cross-border electricity flow through network code

Network codes are traditionally viewed as a set of specific and technical rules for the operation of EU's cross-border electricity networks. The European Commission adopts these acts as implemented or delegated within the constraints outlined in Regulation 2019/943, governing the internal market for electricity. The process for developing network codes involves ACER preparing non-binding framework guidelines that establish objective principles for developing specific network codes,[9] the ENTSO-E and EU DSO entity drafting the network code itself,[10] and ACER revising the proposed network code to ensure that the network code to be adopted complies with the relevant framework guidelines and contributes to market integration, non-discrimination, effective competition, and the efficient functioning of the market.[11] Afterwards, a draft network code is submitted to the Commission for final amendments and its adoption.

Upon European Commission's request, ACER prepared non-binding framework guidelines for the development of the network code for cybersecurity aspects of cross-border electricity flows in 2021. In line with these guidelines, the network code was developed by ENTSO-E in cooperation with EU DSO entity, and subsequently revised by ACER. A draft network code was submitted to Commission in July 2022.[12] As a next step, ENTSO-E and EU DSO entity launched a preparation for the NCCS implementation phase with relevant stakeholders.

The current draft is undergoing a revision by respective regulatory authorities in Member States. The Commissioner for Energy Kadri Simson expected the NCCS to be applicable since January 2024.[13] However, during October and November 2023, Commission published an initiative through *Have Your Say* consultation platform which contained Commission's proposal on delegated regulation on sector-specific rules on cybersecurity to receive feedback, comments and remarks of various stakeholders. Commission's proposal was modified and amended version of the draft network code provided by ACER in July 2022. 36 stakeholders provided their feedback. According to the published initiative the adoption is still planned for the first quarter 2024.[14]

---

8 Cf. European Commission, Digitalising the energy system - EU action plan COM(2022) 552 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552 (accessed on 18 December 2023), 2022.

9 Article 59(4) of the Regulation (EU) 2019/943.

10 Article 59(9) of the Regulation (EU) 2019/943.

11 Article 59(11) of the Regulation (EU) 2019/943.

12 Cf. ACER, ACER submits to the European Commission the revised Network Code on electricity cybersecurity. https://acer.europa.eu/news-and-events/news/acer-submits-european-commission-revised-network-code-electricity-cybersecurity (accessed on 18 December 2023), 2022.

13 Cf. European Commission, Keynote closing speech by Commissioner Simson at ENTSO-E's High-Level Forum on the ‚Future of our grids: accelerating Europe's energy transition' https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_4381 (accessed on 18 December 2023), 2023.

14 Cf. European Commission, EU electricity supply – sector-specific rules on cybersecurity (network code) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EU-electricity-supply-sector-specific-rules-on-cybersecurity-network-code-_

Since network codes are Commission's delegated acts, they have direct effect. Once the Network Code on Cybersecurity is adopted, transmission system operators (TSOs), distribution system operators (DSOs), ENTSO-E, EU DSO entity and other stakeholders within the NCCS scope will have to implement the rules and requirements and act in compliance with them.

Overall, the procedure of preparing the NCCS involves a highly collaborative effort between various stakeholders, including the European Commission, ACER,[15] ENTSO-E,[16] and the Member States' respective regulatory authorities (not only for energy, but also in many Member States special regulators for cybersecurity), to ensure that the code is effective and able to improve cybersecurity and resilience of the electricity system across EU.

As is obvious from the description of the preparatory procedure above, it is highly likely that by the publication of this contribution, the NCCS will have its final form and might even be in effect. Nevertheless, we consider the following discussion on the currently available version as a timely contribution to the upcoming discourse on implementation and future utilization of this innovative regulatory tool.

4. Discussion of the current version and its likely impact

Since the NCCS has not yet been adopted by the Commission, this chapter builds on the draft prepared by the Commission for the purposes of the public consultation process via *Have Your Say Platform*,[17] which is a modified draft prepared for the Commission by ENTSO-E and EU DSO entity and revised by ACER. All subsequent references to articles of NCCS in this contribution refer to this draft version.

The NCCS lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management. It aims to systematically identify digitalized processes critical or with high impact to cross-border electricity flows, assess their associated cybersecurity risks, and determine necessary mitigation measures.

The NCCS is designed to complement already existing cross-sector framework established by the NIS2 Directive and tasks of various already existing institutions and bodies, such as ENISA, NIS Coordination Group, national competent authorities for cybersecurity, national regulatory authorities in energy sectors or CSIRTs. NCCS interacts also with the Regulation (EU) 2019/941 by ensuring that the corresponding measures to address these incidents are adequately incorporated into risk-preparedness plans of entities in the electricity sector and tasks relevant bodies, such as a competent authority for risk preparedness. Drafting documents show EU's intention to ensure a high degree of consistency, coherence, and compatibility with EU energy and cyber law.

Given the dynamic nature of the cybersecurity industry and the multitude of existing methodologies and standards, the NCCS seeks to develop terms, conditions and methodologies. The NCCS also provides governance for cybersecurity risk management, common electricity cybersecurity framework, harmonised cybersecurity procurement requirements, and cybersecurity incident and crisis management.

To stay ahead of emerging cybersecurity trends and anticipate potential risks, the NCCS puts an obligation to certain stakeholders to conduct periodic assessments in the form of the cross-border electricity cybersecurity

en (accessed on 18 December 2023), 2023.

15 I.e. *Agency for the Cooperation of Energy Regulators*, cf. https://www.acer.europa.eu/ (accessed on 21 December 2023), 2023.

16 I.e. *European Network of Transmission System Operators for Electricity*, cf. https://www.entsoe.eu/ (accessed on 21 December 2023), 2023.

17 Available at European Commission, EU electricity supply – sector-specific rules on cybersecurity (network code) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EU-electricity-supply-sector-specific-rules-on-cybersecurity-network-code-_en (accessed on 18 December 2023), 2023, as download link to Draft delegated regulation - Ares(2023)7142081 English.

risk assessments and reports. These reports and assessments are key component of the NCCS framework, which contains very detailed rules on what they should compose of and how they are drafted and approved.

4.1. Identified benefits of NCCS

The main benefit is the very existence of such legislation, as the electricity sector has been rapidly digitalized. It is clear that the smarter the grids and electricity infrastructure in general is, the more vulnerable it gets to cybersecurity threats. On top of that, due to the specificities and complexities of the energy sector, cross-sector cybersecurity framework represented by NIS2 Directive are not suited to effectively mitigate all relevant risks and incidents that might appear during the cross-border electricity transmission.

Harmonised framework for the EU cross-border electricity flows, that the NCCS represents, includes many benefits:

- **Development of a competitive market for digital energy services and digital energy infrastructure that are cyber-secure, efficient and sustainable:** The Clean Energy for all Europeans package adopted in 2019 aims to transform Europe‘s energy systems while maintaining a high level of security, including reinforcing cybersecurity during the process of digital transformation in the energy sector.[18] In addition, adoption of the NCCS was envisaged by the Commission in the Digitalising the energy system – EU action plan.[19] Overall, NCCS represents a significant contribution to the EU‘s objective to build a digitalised, green and resilient interconnected energy system.
- **Setting a Europe-wide standard:** NCCS aims to set an EU standard for the cybersecurity of cross-border electricity flows, which will in consequence help improve cybersecurity in electricity sector across Europe and support development of relevant legislation in Member States, which are currently tackling the implementation of NIS2 into national legislation.[20] NCCS should foster a common minimum electricity cybersecurity level across the EU.
- **Comprehensive and detailed rules:** NCCS contains a broad spectrum of rules beginning with mitigation and preparedness, incident and crisis management, through exercise framework, next regulation of information flows, controls in the supply chain or crisis management and response plans. NCCS also has its own procedural rules and confidentiality regulation.
- **Clear identification of competent stakeholders:** The proposal clearly identifies competent authorities and other bodies responsible for implementation of particular rules and obligations. It also has a “back-up” mechanism stating which authority is responsible for carrying out respective tasks until the competent authority is designated by the Member State.
- **Safer exchange of information:** The proposal aims to establish (via Articles 45 and 46) a legal framework for exchanging cybersecurity-relevant information, which should strengthen collaboration among key stakeholders and increase awareness. More specifically, NCCS will lead to much closer cooperation between ACER and ENISA. It will also further the cooperation between ENTSO-E and EU DSO entity.
- **Cybersecurity procurement:** The NCCS is long missing legal base for many (public) contracting authorities who were not able to fully address possible cybersecurity risks and threats during public procurement procedures due to requirements set by general public procurement law (e.g. general principle of non-discrimination). High and critical-impact organizations shall now be obliged to establish cybersecuri-

[18] Cf. European Commission, Critical infrastructure and cybersecurity https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en (accessed on 18 December 2023), 2023.

[19] Cf. European Commission, Digitalising the energy system - EU action plan COM(2022) 552 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552 (accessed on 18 December 2023), 2022.

[20] Cf. Guidehouse, What the New Cybersecurity Network Code Means for European Utilities https://guidehouse.com/insights/energy/2022/cybersecurity-network-code-european-utilities (accessed on 18 December 2023), 2022.

ty procurement requirements for their ICT products, services and processes. This will benefit the contracting entities by giving them possibility not to let a potentially risky bidder to take part in the procurement or to exclude them from the procurement during the process.

– **Clear legal base for cost regulation:** Article 11 of the NCCS creates very beneficial legal base for recovery of costs of TSOs and DSOs. TSOs and DSOs already invest in more cyber threats resilient grids, however it can be questionable, whether these costs be assessed by the national energy regulator as reasonable, efficient, and proportionate for the purpose of tariff setting and price regulation. Now it is clear that costs used to comply with NCCS will be duly assessed and recovered through network tariffs or by other appropriate mechanisms. However, an issue of cross- border cost sharing between TSOs and DSOs in different Member States remains unaddressed and may arise in connection with regional implementation of NCCS.
– **Reasonable exemptions**: It is quite common that legal acts allow for exemptions from some of their provisions. NCCS is no different and Article 29 allows for granting exemptions to entities listed in Article 2(1) - DSOs, market operators, nominated electricity market operators etc. – they can request a competent authority to grant them time-limited exemption from applying cybersecurity controls, if the costs of the implementation would significantly exceed the benefits or the entity already has a sufficient risk management plan. We see that the way these exemptions are limited in time and scope is beneficial for the entities obliged under NCCS as it takes into account some exceptional circumstances.

Overall, the Network Code on Cybersecurity is an important step towards improving cybersecurity and resilience of the electricity system across the EU.

4.2. Perceived weaknesses of the NCCS

Despite the broad benefits associated with the NCCS, upon subjecting the available version to critical examination, we consider several areas, in which the proposal shows, in our opinion, weaknesses that may limit its impact and effectiveness.

First, the implementation period is extremely long considering the fact that the aim of NCCS is to address current cybersecurity threats. The time for implementation, when all obligations counted altogether, is around 8 years. For example, it can take up to 4 years for the competent authorities to identify and notify high-impact and critical-impact entities, even though such identification/notification of entities with obligations stated in NCCS is crucial for the network code to work. It is very inconvenient for the entities themselves, as they lack an information whether they are to be obliged to comply with the NCCS or not.

Second, there is also a lot of interdependencies in different stages and processes, meaning if one process is delayed, it results in the delay of the following one. In different words, if one part of the chain breaks or is delayed, it influences the rest of the chain. One example is connected to the aforementioned identification of high-impact and critical-impact entities according to Article 23 of NCCS; national competent authorities shall in doing so take into consideration threshold established in the *Union-wide cybersecurity risk assessment report* pursuant to Article 18(5). This report in itself has a number of procedural checks that involve ENTSO-E, EU DSO entity, ACER, ENISA and the Commission. However, it also cannot be performed and finalized without the *Cybersecurity risk assessment methodology*, prepared under Article 17, which has to previous to that be approved in accordance with the procedure outlined in Article 8 (5–8) by the national competent authorities.

Third, comment must also be made on the legislative technique of the draft. The draft is supposed to be quite technical and such type of legal acts are always rather unfriendly to the reader, however, the nature of NCCS does not justify its lack of clarity. The addressee of the act gets lost in enormous number of interconnected links to different provisions of the network code forcing the addressee to repeatedly go back to check on the linked provision. This makes the act very user-unfriendly, which is certainly a major obstacle as many provi-

sions are addressed not only to the competent authorities, but to the obliged entities, making it complicated for them to identify and interpret their obligations. On top of that there are several provisions, e.g., Article 4(3) or 36(7), that allow for delegation of certain tasks. This may cause further uncertainties for the obliged entities, who have limited means to be aware of such delegation taking place or not.

Another weakness can be perceived in the excessive amount of planning obligations (see Chapter II *Risk assessment and identification of the relevant cybersecurity risks* in particular). Obliged entities shall prepare methodologies and risk assessments on different levels, all of them being subject to approval of numerous authorities. Having look at what all these documents shall assess and contain, the question arises whether it is actually necessary and how overlaps will be avoided if, e.g., regional cybersecurity risk assessment report should take into account both Union-wide and Member State level risk assessment reports. We find problematic the unification of approval terms and conditions, methodologies or plans. The already mentioned Article 8 sets procedure for approval of terms, conditions and methodologies envisaged by the NCCS by the relevant competent authorities. This mechanism build on coordination and unification can easily slow down effective implementation of the network code.

The alignment of the NCCS with the provisions of NIS2 Directive is obvious intention and goal of the legislator, but the current version still falls short in this regard. Parallel use, parallel supervision and parallel incident reporting under both the NCCS and the NIS2 Directive need to be duly avoided. Given that the NIS2 Directive builds in the Member States on an already established national architecture of cyber security supervision, transparent and coherent approach for the obliged entities to the compliance with the NCCS is achievable only if such duplications and fragmentation of requirements can be duly avoided. This risk of duplication and overlapping can be seen for example in Article 28 and 31 to 33. These NCCS provisions lack clarification of the relationship to the NIS2 requirements, and therefore represent a risk of overload of obligations and different approaches for the obliged entities. Also, NIS2 Directive itself will bring (considering the timely national implementation) much faster harmonisation of many cybersecurity related questions than can be envisaged under the NCCS procedures outlined above. As another example can be used the above-mentioned proposal of Cyber Resilience Act, which also sets rules for security of supply chains and with much broader scope and, what is more important, high probability of entering into force sooner than respective provisions of NCCS.

Finally, the enforcement mechanism in the proposal is not clearly established, which may further complicate ensuring full compliance with the rules across Europe.

It is additionally worth noting that the NCCS obviously focuses on improving cybersecurity and resilience of the electricity system and electricity flows across Europe, but it does not cover all aspects of cybersecurity in the energy sector since the Regulation (EU) 2019/943 cannot focus on cybersecurity in gas industry. We believe that similar rules should be implemented in connection to cross-border gas flows taking into account gas sector specifics. Commission already aims to adapt the gas system to new risks, such as cyber-attacks by intention to propose a delegated act on the cybersecurity of gas and hydrogen networks. However, for this purpose the Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas supply needs to be amended.[21]

To conclude our analysis, despite some more or less avoidable weaknesses highlighted above, NCCS is a major step in the right direction, which can largely improve cybersecurity in the European electricity systems and by consequence encourage overall progress in this regard in the energy sector as a whole, even though it may take longer than would be suitable.

[21] Cf. Guidehouse, What the New Cybersecurity Network Code Means for European Utilities https://guidehouse.com/insights/energy/2022/cybersecurity-network-code-european-utilities (accessed on 18 December 2023), 2022.

5. Conclusion

In our contribution, we aimed to discuss the soon to be finalized Network code for cybersecurity, its benefits and limits. It is a welcomed contribution to the enhancement of cyber security in the energy sector, as it contributes to maintaining security and resilience while taking into consideration electricity sector specifics and shall set EU-wide cyber security standards. It shall provide comprehensive and detailed rules and clear identification of competent stakeholders. NCCS includes rules ensuring safer exchange of relevant information and also long missing legal base for cybersecurity procurement rules. Last but not least, NCCS provides clear base for cost regulation for regulated entities.

On the other hand, we also identified some more or less serious weaknesses. In particular, we perceive as problematic the very long implementation period for determining the requirements, when we are already in situation, when the foreseen measures are seriously needed. However beneficial the rules can be, they have no use, if they come into effect only after several years from publication of the network code. There is also a lot of interdependencies in different stages and processes, setting the stage for possible delays. We further find the NCCS to be very planning-heavy with significant risks of unnecessary overlaps. Worth noting is also the user-unfriendly legislative technique with high number of cross-references. This makes the network code very hard to read and understand even for expert users. Lastly, caution is recommended with regard to several unclear alignment with NIS2 Directive and other legislation.

It can be concluded that despite some potentially major weaknesses, the NCCS provides a crucial basis for comprehensive, detailed and harmonised rules on cybersecurity for cross-border electricity flows and represents a needed piece of legislation in the electricity sector.