THE ROAD TOWARDS A LEGAL FRAMEWORK FOR CYBERSECURITY APPLICABLE TO THE EUROPEAN SMART GRID FOR ELECTRICITY

František Kasl / Anna Blechová

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

Anna Blechová, 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: 458594@muni.cz

Keywords: ***Energy Sector, Electricity Distribution, Cybersecurity, Smart Grid, EU Law***

Abstract: *The European energy sector faces a rising vulnerability to cyberattacks, posing a significant threat to modern societies due to its interconnected nature with critical infrastructure. This fragility could result in substantial physical and economic harm and be exploited for geopolitical purposes, as it is possible to see with the war in Ukraine. While digitalization enhances efficiency, it also exposes vulnerabilities. Recognizing the urgency of protecting critical energy infrastructure, a new European legislative framework is being established. This contribution focuses on examining the new regulatory framework and identifying persisting challenges for development of smart grids for electricity.*

1. Introduction[1]

The European energy sector is facing an escalating vulnerability to cyberattacks, rendering cybersecurity a paramount concern for the industry. Furthermore, cyberattacks on electricity systems in particular pose a critical threat to all facets of modern societies, given the interconnected nature of the electricity power grid with other vital infrastructure and services.[2] The fragility of Europe‘s digital security and global energy interconnections could have a profound impact on the lives of its citizens and lead to significant physical and economic harm.[3] Moreover, the vulnerabilities of energy sector could be also used as an tool to achieve geopolitical goals as was unfortunately highlighted by actions accompanying the war in Ukraine at least since early 2022. As such, the electricity systems are becoming increasingly attractive targets for hackers.[4] This is supported by the fact that, in 2022, 10.7% of cyberattacks were directed at the energy industry, as reported by the X-Force Threat Intelligence Index 2023.[5]

Moreover, the rapid proliferation of connected energy resources and devices is expanding the potential surface for cyberattacks. The rise in connectivity and automation across the electricity system is heightening

[1] This article is based upon the grant of the Technology Agency of the Czech Republic, THETA programme, Secure power flexibility for grid control and market purposes (SecureFlex) - TK01030078.

[2] Cf. IEA, Enhancing cyber resilience in electricity systems https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (accessed on 18 December 2023), 2021.

[3] Cf. Nelson/Romero, Why Europe’s energy industry is vulnerable to cyber-attacks https://ecfr.eu/article/why-europes-energy-industry-is-vulnerable-to-cyber-attacks/ (accessed on 18 December 2023), 2022.

[4] Cf. Jack, Europe’s grid is under a cyberattack deluge, industry warns https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/ (accessed on 18 December 2023), 2023.

[5] Cf. Bonderud, 2022 industry threat recap: Energy https://securityintelligence.com/articles/2022-industry-threat-recap-energy/ (accessed on 18 December 2023), 2023.

cybersecurity risks.[6] The adoption of smart grids and smart meters is on the rise throughout Europe, but this digitalization of the electricity subsector also exposes elements of the critical infrastructure to new forms of vulnerabilities. It is undeniable that the energy sector requires specific and effective measures supported and enforced by appropriate regulation to safeguard critical energy infrastructure against cyberattacks. This necessity was also highlighted by the Special Eurobarometer 492, conducted in 2019, which revealed that 86% of EU citizens support increased cooperation on cybersecurity in the energy sector among EU countries to ensure access to secure energy.[7]

The electricity sector has a unique set of operational conditions and requirements, vulnerabilities, and solutions compared to other sectors.[8] Admittedly, there is a regulatory framework in place for the electricity subsector in the form of broadly harmonizing NIS Directive[9] and sector-specific Regulation on risk-preparedness in the electricity sector (EU) 2019/941.[10] However, the year 2023 has seen a significant progress towards new regulatory framework setting cybersecurity requirements to critical infrastructure and essential services. It includes the NIS 2 Directive[11] and the Critical Entities Resilience Directive (CER).[12] On top of that, there are additional acts in the legislative process that will further enhance the complexity of the landscape, such as the Network Code on Cybersecurity or the European Cyber Resilience Act (CRA).[13]

In summary, the increasing interconnection and automation of the European energy sector, coupled with the ongoing threat of cyberattacks, make cybersecurity a pivotal concern for the industry. There is a lot of activity towards this goal and consequentially, the traditionally slow-paced landscape of energy sector is suddenly forced to evolve much more rapidly than was the case in previous decades. This applies not only to the technology used across this industry, but given the overall transition of the energy sector in the EU towards carbon-free future, a lot of the changes are based on strategic and political decisions, enforced through regulatory obligations and requirements, rather than free market forces and gradual changes in line with normal asset renewal and upgrade.

In this contribution, we aim to investigate this new enhanced cybersecurity regulatory landscape with focus on consequences and requirements for entities in the electricity subsector creating the increasingly interconnected (and interdependent) smart grids in the EU (i.e. transmission system operators (TSOs), distribution system operators (DSOs), smart grid communication operators, energy aggregators, smart metering providers etc.).[14] During the analysis, we will focus on the question, if there are critical cybersecurity challenges on the current EU trajectory towards smart grids for electricity that are not suitably reflected in the current or upcoming regulatory framework? As for methodology, we will employ a doctrinal analysis to explore relevant policy context and smart grid trends. The core effort will be aimed at an examination of the respective legal acts and the prospective incompatibility with the identifiable trends or needs in the EU electricity subsector.

---

6 Cf. IEA, Enhancing cyber resilience in electricity systems. https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (accessed on 18 December 2023), 2021.

7 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.

8 Cf. IEA, Cyber resilience. https://www.iea.org/reports/power-systems-in-transition/cyber-resilience (accessed on 18 December 2023), 2023.

9 Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 18 December 2023).

10 Regulation (EU) 2019/941 of 5 June 2019 on risk-preparedness in the electricity sector. https://eur-lex.europa.eu/eli/reg/2019/941/oj (accessed on 18 December 2023).

11 Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) https://eur-lex.europa.eu/eli/dir/2022/2555 (accessed on 18 December 2023).

12 Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 18 December 2023).

13 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).

14 Cf. European Commission, Smart Grids in the European Union. https://setis.ec.europa.eu/smart-grids-european-union_en (accessed on 18 December 2023), 2022.

The contribution is structured as follows: Section 2 provides a summary overview of the relevant legal framework with focus on provisions or instruments that will be discussed further in Section 3. In Section 3, we identify challenges from the cybersecurity perspective with significant impact on the development of smart grids in the EU and analyse, if the current or upcoming regulatory framework provides adequate response. Section 4 contains a short summary of the main conclusions.

2. The emerging complex EU cybersecurity framework for electricity subsector entities

Several recent and upcoming cybersecurity-focused legal acts are poised to have a profound impact on the energy sector at various levels. First, we will address the NIS 2 Directive and outline the relevant changes it imposes on the entities revolving around the smart grid for electricity, especially in comparison to the NIS Directive. Subsequently, we will examine the CER Directive. Both of these harmonising acts should be transposed into the national laws of the EU Member States during the first half of 2024, as their main provisions shall be applicable starting with 18 October 2024. Additionally, we will examine the Network Code on Cybersecurity and identify provisions of the proposal for Cyber Resilience Act relevant to the discussion that follows.

2.1. NIS 2 Directive

The NIS 2 Directive was published on 27 December 2022 and each Member State now has to transpose the new rules into the national legislation. This means that although the basic regulatory framework has been established, Member States can still partially modify and shape the rules in their national legislations. This is in fact necessary in the context of the electricity subsector, as there are significant differences between the Member States in the composition of the involved entities, achieved progress towards smart grid or decentralization. Furthermore, the role and capacity of the national energy regulatory authority or (more often) several such authorities with not always well-defined boundaries of powers and scope differs throughout the EU. This is particularly true for the relatively new context of cybersecurity requirements, where the role of the national energy regulatory authority and the national cybersecurity authority overlap and the need for cooperation is essential, given that the specifics of the energy sector and the specific of the cybersecurity perspective need to be both considered.

NIS 2 Directive sets minimum rules for the coordinated regulatory framework, establishes mechanisms for effective cooperation among responsible authorities across Member States, updates the list of sectors and activities subject to cybersecurity obligations, and provides effective remedies and enforcement measures crucial for the NIS 2 Directive‘s effective enforcement. Its aim is to enhance cybersecurity capabilities across the EU, mitigate threats to network and information systems used to provide essential services in key sectors, and ensure the continuity of such services during incidents. It is therefore by far not limited to energy sector, but energy sector is one of the core areas of focus, highlighted in Annex I, where electricity subsector is identified as the first sector of high criticality.

One of the primary changes introduced by the NIS 2 Directive in comparison to the NIS Directive is the differentiation of obliged entities into two categories: “essential entities” and “important entities” (Art. 3). This distinction reflects the extent to which they are critical within their sector or the type of service they provide, as well as their size. Member States should create a list of entities falling within the scope of each of these categories. As a result, the NIS 2 Directive introduces a dual-track security regime for providers, with varying levels of obligations. This relates to the most noticeable change with regard to energy sector, i.e., a major the expansion of the scope of energy sector entities to which the legislation shall apply in comparison to the NIS Directive regime. The NIS 2 Directive shall apply not only to large critical enterprises in electricity production

or distribution, but also to many small and medium-sized businesses involved in the functioning of the smart grid and decentralized energy system.[15] The scope of regulation extends to independent flexibility aggregators, demand side response providers, energy storage service providers or charging point operators. Furthermore, the obligations expand beyond electricity producers and distributors to include all critical infrastructure subcontractors. Depending on the size and role of the entity, it shall be classified as "essential" or "important".

As for specific obligations, the NIS 2 Directive mandates that energy companies implement appropriate technical and organizational measures to prevent, detect, and respond to incidents that could impact the security and continuity of energy supply. This encompasses measures to protect critical infrastructure, ensure data protection and privacy, and maintain the availability of energy services.[16]

2.2. Critical Entities Resilience Directive

The goal of the CER Directive is to ensure cross-border cooperation for critical entities and to enhance their resilience. The Directive aims to achieve this goal by requiring Member States to designate or establish competent authorities and a single point of contact to ensure effective cooperation with other Member States and the Critical Entities Resilience Group.[17] The CER Directive lays down harmonised rules allowing for a consistent identification of critical entities across the EU, while also allowing Member States to adequately reflect the role and importance of those entities at the national level.

The CER Directive aims to reduce divergences in the resilience requirements of critical entities across the EU. Member States are required to support critical entities, including those that qualify as small or medium-sized enterprises, in strengthening their resilience, in compliance with Member State obligations laid down in this Directive, without prejudice to the critical entities' own legal responsibility to ensure such compliance and, in so doing, prevent excessive administrative burden. The CER Directive also aims to facilitate cooperation between the competent authorities under this Directive and the competent authorities under the NIS 2 Directive for the purposes of information sharing on cybersecurity risks, cyber threats and cyber incidents and non-cyber risks, threats and incidents and the exercise of supervisory tasks.

The CER Directive, similarly to the NIS 2 Directive, identifies the electricity subsector in its Annex as the first of the critical sectors that require cross-border cooperation and enhanced resilience. The competent authorities and single points of contact established under this Directive are required to have the necessary powers and resources to carry out their tasks effectively. The single points of contact are required to submit a summary report every two years on the notifications they have received, including the number of notifications, the nature of notified incidents, and the actions taken. Each critical entity shall designate a liaison officer or equivalent as the point of contact with the competent authorities. The Commission shall adopt non-binding guidelines to further specify the technical, security and organisational measures that should be taken in this regard by the identified critical entities.

2.3. Regulation (EU) 2019/941 and the Network Code for Cybersecurity

The NIS 2 Directive and the CER Directive are general frameworks applicable to multiple sectors. Therefore, sector-specifics need to be delegated to additional legal acts, or more often to secondary acts and guidelines adopted by the Commission. Currently, the Regulation (EU) 2019/941 on risk-preparedness in the electricity sector is the most significant sector-specific act to be considered. This regulation addressed the need for a

[15] Cf. Centre for Cybersecurity Belgium, The NIS 2 Directive: what does it mean for my organization? https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization#_Toc128118854 (accessed on 18 December 2023), 2023.

[16] Cf. NIS2 Directive, Energy Sector https://nis2directive.eu/energy/ (accessed on 18 December 2023), 2023.

[17] Cf. The Critical Entities Resilience Directive (CER). https://www.critical-entities-resilience-directive.com/ (accessed on 18 December 2023), 2023.

common approach to risk-preparedness. It requires Member States to develop and maintain risk-preparedness plans, conduct risk assessments, and cooperate with other Member States and the European Commission in the event of an electricity crisis. It also emphasizes the importance of information exchange and transparency in crisis situations.

Furthermore, Article 59(2)(e) of Regulation (EU) 2019/943 on the internal market for electricity[18] empowers the Commission to adopt delegated act on sector-specific rules for cybersecurity aspects of cross-border electricity flows. This resulted in the preparation of the Network Code on Cybersecurity (NCCS),[19] which lies down rules on common minimum requirements, planning, monitoring, reporting and crisis management in this context. The NCCS is designed to complement the existing framework with providing more specific requirements and procedures tailored for the trans-border vulnerabilities of increasingly interconnected smart grids in the EU. As such, this delegated act should be finalized and come into force in 2024,[20] however, the procedures foreseen within are likely to take years to reach the intended state and effect. The adoption of terms and conditions, methodologies and plans that shall constitute the backbone of the measures is complex, involves numerous stakeholders (TSOs, ENTSO-E, EU DSO entity, ACER, ENISA as well as the Commission) and the implementation periods (4–8 years with all steps considered) are not aligned with the urgent need for action highlighted by the state affair on the cyber security front in the electricity subsector, as presented in the introduction to this contribution.

2.4. Proposal of Cyber Resilience Act

The CRA proposal aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's life cycle.[21] The draft regulation introduces mandatory cybersecurity requirements for the design, development, production, and making available on the market of products with digital elements. The Regulation sets out four specific objectives: to increase the overall level of cybersecurity of all products with digital elements placed on the internal market, to introduce objective-oriented and technology-neutral essential cybersecurity requirements for these products that apply horizontally, to ensure a high level of cybersecurity of products with digital elements, and to facilitate the assessment of conformity with the requirements laid down in this Regulation. The horizontal cybersecurity rules laid down by this proposal are not specific to sectors or certain products with digital elements, but sectoral or product-specific rules are envisaged by this Regulation.

Enhancing the cyber resilience of electricity systems warrants tailored policies and strategies. Effective policies need to look beyond bulk utilities and consider the entire electricity chain, including supply chains. The fundamental principles of cyber resilience, such as embedding a culture of cyber hygiene and implementing risk management strategies, are generally applicable across all sectors and industries. However, the application of these principles needs to be tailored to account for sector-specific characteristics and needs.[22] In the electricity subsector, in the context of modern smart grid designs, these include real-time requirements for

[18] Regulation (EU) 2019/943 of 5 June 2019 on the internal market for electricity (recast) https://eur-lex.europa.eu/eli/reg/2019/943/oj (accessed on 18 December 2023).

[19] 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, available at link *Draft delegated regulation - Ares(2023)7142081 English*.

[20] 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.

[21] Cf. Proposal 15.9.2022, Cyber Resilience Act. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 (accessed on 18 December 2023), 2023.

[22] Cf. IEA, Enhancing cyber resilience in electricity systems. https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (accessed on 18 December 2023), 2021.

and expectations of very high availability, communication with external stakeholders, and the need for tailored policies and strategies. These are often not in place at this time and adoption of the CRA proposal could therefore be a vital incentive towards their creation. The CRA proposal mandates security-by-design by creating a list of essential cybersecurity requirements for manufacturers, importers, and distributors of connected devices and services to comply with through certification, reporting, and conformity assessments. This covers the planning, design, development, production, delivery, and maintenance of products with digital elements. It also requires manufacturers to improve the security of products with digital elements since the design and development phase and throughout the whole life cycle.[23]

The expected impact of the CRA proposal on the electricity subsector will likely be implicit rather than explicit. Nevertheless, with the increasingly connected nature of the smart home solutions and multitude of elements of decentralized power generation at the points of consumption, it will still have likely a significant impact. The Regulation will apply to all products that are connected either directly or indirectly to another device or network, and it aims to increase the overall level of cybersecurity of all products with digital elements placed on the internal market. Therefore, it will be of crucial relevance for the edge elements of the smart grid, which are currently over outside the scope of the previously mentioned regulatory acts. This is due to their fragmented ownership, diverse origin and multitude of use case scenarios. With the increasing interaction of the elements on all levels of the smart grid, the edge devices will play increasingly important role even for the traditionally core activities and responsibilities of the DSOs and TSOs, given that their analytics, reaction and data flows will be unavoidably linked and affected with these elements on the edge.

3. Discussion of the challenges ahead

The transition of the electricity subsector in the EU as such is subject to a number of analyses and strategies by the Commission, ACER,[24] ENTSO-E,[25] EU DSO entity[26] and various other organisations or research bodies, which is mainly due to the fact, that the main impulse for this transition does not have technological or market origin, but it is based on the EU-level strategy for carbon-free economy[27] and subsequent political and legislative measures to "enforce" this transition on the EU economy as a whole and electricity subsector in particular. Out of these numerous sources, there are two that we would like to pinpoint for the subsequent discussion. *Smart Grid Key Performance Indicators: A DSO perspective*[28] is a 2021 report by ENTSO-E and four DSO associations (CEDEC, E.DSO, EURELECTRIC and GEODE), providing on one hand comprehensive summary of the smart grid concept and technical challenges associated with transitioning to this modern design of the electricity grid with increased connectivity and data layer. On the other hand, it gives an insight into the scope of challenges set for the TSOs and DSOs in this process. These entities will need to adopt many new business processes and policies that transform the core of their operations. Namely, the collaboration and data exchange with other TSOs and DSOs nationally, but also across borders will need to be much more extensive, robust and often real-time or near time, so in effect automated.

---

[23] Cf. European Commission, Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act (accessed on 18 December 2023), 2023.

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

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

[26] I.e. the European entity for the cooperation of electricity distribution system operators (DSOs) in the European Union, cf. https://eudsoentity.eu/ (accessed on 21 December 2023), 2023.

[27] Communication from the Commission ‚Fit for 55': delivering the EU's 2030 Climate Target on the way to climate neutrality. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0550 (accessed on 18 December 2023).

[28] Cf. Eurelectric, Smart Grid Key Performance Indicators: A DSO perspective. https://www.eurelectric.org/publications/smart-grid-key-performance-indicators-a-dso-perspective (accessed on 18 December 2023), 2021.

These key players in the electricity subsector will be required to collaborate to much larger degree than previously (due to the interconnected, interdependent nature of the new design of the grid) on real-time network operations as well as network operations planning; exchange all necessary information related to long-term network investment planning or to generation assets and demand side response for the daily operation of their networks; as well as cooperate to achieve a coordinated approach to resources. This is due to the change in available tools for TSOs and DSOs in load management (i.e., stability of the grid and quality of the electricity provided) caused by decentralized and partially hard-to-predict electricity production (due to increasing role of spatially distributed solar and wind energy sources). On top of that, the TSOs and DSOs will more than previously take on the role of "gatekeepers" or operators of the infrastructure, which is used by other entities for additional business aims or operations (similar to the telecommunication sector or providers of internet connection infrastructure). These entities, which may include e.g. independent flexibility operators, operators of charging stations or peer-to-peer electricity trading platforms, will require additional layers of data flows and collaboration, in order to maintain balance of the grid and permit the emergence of these new elements on the electricity market. The increasing cross-border connectivity then adds another layer of complexity due to new contact points between similar-but-not-the-same electricity markets and grids. All this will be reflected not only in the new demands for ICT capacities, but it will also present new cybersecurity threat landscape.

As it was highlighted in Chapter 2, the above-mentioned legal framework is fully reflecting this transition and it is setting a multitude of new or more comprehensive and broadly applicable obligations for the electricity subsector entities. This is certainly step in the right direction, but the sheer complexity of the sector structure and regulation[29] is often seemingly intentionally further multiplied by the new demanding obligations for documentation, analyses, methodologies, rules and reports that likely overlap on various levels.[30] Ploughing through all these requirements will add even more burden on the obliged entities. Thus, it is crucial to promote a careful and considerate approach from the competent regulatory authorities. This approach will prevent the resources of the entities from being stretched too thin due to excessive documentation and endless procedural formalities.

Another substantial concern arises from the scarcity of resources: the shortage of experts. Securing cybersecurity professionals is inherently challenging, particularly those possessing the specific skill sets and contextual understanding pertinent to the electricity subsector.[31] The pressing transition and sudden surge in demand for these specialists across the EU's electricity subsector, which previously allocated only limited resources for cybersecurity, intensify the challenge. Historically, these systems were obscure and primarily shielded from the broader internet for protection. Consequently, capacity building emerges as the primary bottleneck in these efforts.

Extensive documentation and collaboration obligations may help in rising the bottom threshold and increasing thereby the state of cyber security in the electricity subsector overall, but it can also slow implementation of the measures at critical points. If the regulatory framework envisaged commonly agreed standards or practices, then obliged entities may refrain from committing to certain technical solution or process before such agreement is met. This may result in delayed implementation of the required measures that would be suitable from the current threat perspective, which was indicated in the introduction. This is made more critical in the electricity subsector, which traditionally works on rather long product cycles (most elements in the grid infrastructure get systematically renewed in the cycles consisting of decades rather than years).

[29] The electricity subsector is subject to very robust regulatory framework due to its critical societal nature.

[30] These overlaps may be to a part unavoidable, as they likely reflect the diversity of the electricity sectors in the individual Member States, to which the "one-size-fits-all" provisions in the EU-level legislation shall be applied.

[31] Cf. Stupp, European Electricity Sector Lacks Cyber Experts as Ukraine War Raises Hacking Risks. https://www.wsj.com/articles/european-electricity-sector-lacks-cyber-experts-as-ukraine-war-raises-hacking-risks-11670605079 (accessed on 18 December 2023), 2023.

The investment perspective is well described in the 2021 report *Connecting the dots: Distribution grid investment to power the energy transition*[32] from E.DSO, Deloitte and eurelectric. It summarizes that the smart grid transformation is a major investment operation within these product cycles of the grid elements, which needs to take place soon on a large scale, if the goals of the transformation to carbon-free economy should remain feasible. There is a major transformation on the part of energy sources and energy consumption, which needs to be reflected in the investments into the grid. According to the study, these will require 375–425 billion EUR investment in the grid during 2020–2030 for a cost-efficient scenario of load flexibility measures, which represents 50–70% increase in annual investment in power distribution grids compared to 2015–2019 period.[33] These numbers are from the pre-Ukraine war perspective, so current outlook may be even more challenging. Also, these costs are not specifically taking into consideration cybersecurity. Nevertheless, as evident from the EU Cybersecurity approach outlined in Section 2, fulfilling all mandated obligations incurs expenses. In a landscape characterized by rapid movement and change, sustaining pressure to enforce the envisaged enhanced cybersecurity requirements becomes challenging. This challenge is compounded by potential gaps and limitations in the enforcement capacity of the individual regulatory authorities mentioned earlier.

4. Conclusion

There is an obvious increase in the dynamic of legislative as well as regulatory requirements with regard to cybersecurity of entities in the energy sector, which is progress in the right direction. However, the emerging framework seems to be excessively built on complex and Kafkaesque procedural requirements, which will take a lot of time and lot of resources to implement. This will possibly overburden the already hard-to-get cybersecurity personnel in electricity subsector and are likely to collide with other priorities of the obliged entities. Furthermore, without well-balanced enforcement involving guidance, support and decisive actions in case of non-compliance by regulatory authorities, the goal of robust cybersecurity landscape in the electricity subsector might remain frustratingly out of reach.

[32] Cf. eurelectric, Connecting the dots: Distribution grid investment to power the energy transition https://www.eurelectric.org/connecting-the-dots (accessed on 18 December 2023), 2021, Available under *Download slide deck*.

[33] *Ibid*., p. 36.