energies

MDPI

Article

Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU

Michał Krzykowski [1,2]

[1] Department of Economic & Commercial Law, Faculty of Law & Administration, University of Warmia and Mazury in Olsztyn, Obitza 1, 10-725 Olsztyn, Poland; michal.krzykowski@uwm.edu.pl

[2] Climate & Energy Laboratory, Centre for Antitrust and Regulatory Studies, Faculty of Management, Warsaw University, Szturmowa 3, 02-678 Warszawa, Poland

Abstract: Due to the strategic nature of the energy sector, legal solutions to protect cross-border electricity and gas connections will be of particular importance. The author realizes that at the present stage of development, the cross-border impact may also be manifested by generating units (e.g., wind farms) or even end users themselves. The lack of harmonized regulations in this area may not only lead to limitations in the physical supply of electricity and gas, but also affect future investment decisions regarding, for example, new generation capacities. In a broader aspect, it will delay, and in the extreme case prevent, the achievement of the objectives resulting from the EU energy policy, in particular integration within the single energy market. In this article, the author identifies devices and entities responsible for energy infrastructure that should be classified as necessary for the functioning of the single energy market. The research includes the analysis and evaluation of regulations governing cybersecurity in the energy sector, taking into account the interdependencies within, intersectoral and cross-border. In addition, the author refers to the need to introduce individual legal solutions regarding the protection of energy infrastructure.

Keywords: energy sector; cybersecurity; policy and decision making; critical infrastructure

Citation: Krzykowski, M. Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU. *Energies* **2021**, *14*, 7836. https://doi.org/10.3390/en14237836

Academic Editors: Peter Burgherr and Manuela Tvaronavičienė

Received: 28 October 2021
Accepted: 18 November 2021
Published: 23 November 2021

1. Introduction

In view of the progressing digitization & digitalization of the internal market, as well as the changing threat landscape, the issue of energy infrastructure protection has become incredibly pertinent to uninterrupted trade and investment in the energy sector. In essence, digitization encompasses a number of activities aimed at increasing the availability of the internet and online resources, as well as incorporating electronic processes into public administration. Digitalization, on the other hand, relates to converting analogue materials into digital form by means of scanning or photography. This process usually involves the creation of various types of metadata, as well as the collecting, structuring, processing, archiving, managing, exchanging, protecting, and sharing materials/data via networks. Digitalization is therefore a narrower concept than digitization, and is, in fact, a component of digitization (which is aimed at the development of e-sources and e-services) [1,2]. Indeed, there is no doubt that energy transformation—based on the development of distributed renewable energy, increased energy efficiency, demand flexibility, energy storage, and the combining of sectors—will be mostly driven by digital solutions (under the general umbrella of digitalization). These technologies form one of the pillars of modern energy policy of the EU (as well as the USA, China, and others), which is based on three fundamental principles—the three "D"s of decarbonization, digitalization, and decentralization [3]. These factors have sparked a transition from the existing European energy network into a smart grid which should better match the actual supply and demand for electricity/natural gas [4–6]. Its multi-faceted and interconnected nature means that the energy sector requires legal solutions that would facilitate effective security at each stage

of the electricity/natural gas supply chain (disrupting one component of the chain may affect not only the operability of the sector in question, but also cause ripple effects on other areas of the economy). This problem is further exacerbated by the fact that cybersecurity incidents have been increasingly taking place across borders, whereas the jurisdictions of—and policy responses by—cybersecurity authorities are predominantly national. Thus, such incidents could disrupt the provision of essential services across the Union. This risk seems to have become even more serious due to the COVID-19 pandemic. After all, there is no denying that the pandemic has forced even more areas of human activity to migrate to the cybersphere [7]. That is why there needs to be an effective and coordinated approach to response and crisis management at Union level, building on specific policies and wider instruments for European solidarity and mutual assistance [8].

In the article, the author attempts to identify potential and actual threats to the energy sector arising from cyberspace and indicates legal solutions aimed on preventing and eliminating their effects. The basic thesis is the assumption that cybersecurity is a condition for the cross—border trade and investment in the energy sector on the EU level.

As part of such a thesis, the author make an attempt to answer defined questions:

- what are the reasons for cyber—protection of energy infrastructure,
- what are the legal criteria of identifying energy infrastructure exposed to cyber attacks or incidents,
- why there is a necessity to introduce regulations at the EU level,
- do the legal solutions ensure a sufficient level of cybersecurity,
- are the horizontal regulations sufficient to ensure cybersecurity in the energy sector,
- what are the interdependencies within and between sectors in the context of the cybersecurtity in the energy sector,
- will the proposed legal solutions ensure more effective cyber protection of energy the infrastructure.

2. Materials and Methods

The present paper adopts the dogmatic-legal method as its primary mode of analysis, which draws on the results of linguistic (grammatical), systemic, and teleological (purposive) interpretation. These methods will be used to analyze primary and secondary sources of EU law, international law, and European Commission soft law. The paper also bases on opinions of experts on the legal doctrine regarding the subject at hand. The linguistic interpretation will particularly focus on secondary EU legislation on cybersecurity in the energy sector. Moreover, these provisions will also be subjected to systemic interpretation in order to determine their proper meaning on the basis of their location in the system of law and interpreted according to their intended objectives.

3. Cybersecurity as a Concern for the Energy Sector

As expressed by the EC in a 2013 communication, from a political viewpoint "An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies . . . " [9]. On the economic side, it expands current market outlets and enhances the efficiency and operativity of the supply chain. However, this transition also increases the risk of unwanted actions that could disrupt the market by cutting off the supply of essential services such as water, healthcare, electricity, natural gas supply, or telecommunications. Such occurrences can have various causes, including criminal, politically motivated, terrorist or state-sponsored actions, as well as natural disasters and unintentional mistakes [9]. The cyberspace-related threat is intensified by the blurring of the border between cybercrime and traditional crime. Furthermore, identifying the perpetrators and bringing them to justice can be extremely difficult. The last few years have seen a rise in the number of incidents and cyber threats to cybersecurity. According to

the EC communication, the economic impact of cybercrime rose fivefold from 2013 to 2017, and could further quadruple by 2019. Ransomware has seen a particular increase, with the recent attacks reflecting a dramatic rise in cyber-criminal activity [10]. An "incident" is "any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems", Article 4 (5) of the proposed NIS 2 Directive. The proposed NIS 2 Directive clarifies and extends the term "incident" as used previously in the NIS Directive (Article 4 (7)), mainly by directly linking an event compromising the transmission or processing of data with the related services offered by network and information systems. According to Article 2 (8) of Regulation 2019/881/EU, a "cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons. According to Article 2 (1) of Regulation 2019/881/EU, "cybersecurity" means "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" [11].

As far as the energy sector itself is concerned, the most serious of these activities have involved disruptions to the electricity grid, the gas grid, gas pipelines, and oil refining facilities. For example, an infection of the American electricity system with malware (Blaster Worm) in 2003 caused a cascading effect, resulting in a power outage that affected 50 million customers in North America (North-eastern blackout, USA and Canada, 2003). In 2008, the Baku-Tbilisi-Ceyhan (BTC) pipeline in Turkey suffered an explosion due to a cyber attack on the line's control and safety systems. The attack caused increased pressure in the pipeline, which in turn led to an explosion. In 2021, Colonial Pipeline, an oil pipeline system stretching from the Gulf of Mexico up to New York, was targeted by an attack that encrypted the computerized system for managing the pipeline, hindering gasoline and motor oil supplies to the USA East Coast. Although most such attacks did not directly affect the EU's energy infrastructure, their potentially cross-border scope and cascading effects may constitute a serious potential driver of risk for the establishment of a single energy market unless a coherent strategy is developed to counteract them (effective identification, protection and appropriate countermeasures to address the risks involved). According to the 2018 Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector, commissioned by the EC [12], hypothetical disruption scenarios can involve a number of energy system components. These include IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) such as firewalls, which form the backbone of ICT protection systems. A successful infection of these systems would enable the attacker to obtain access rights for all crucial elements of the energy system. For example, a threat agent gaining access to the internal network of a power generator can then infect the systems of distribution/transmission grid operators, and thus almost the entire energy supply chain. This is made even more likely by the fact that Industrial Control Systems (ICS) of generators are often not designed for internet connectivity, and thus tend to be highly vulnerable to potential incidents. SCADA (Supervisory Control and Data Acquisition) systems, which happen to be widely used in the energy sector, are particularly susceptible. The system is designed to integrate the energy network and optimize its operation, with its main functions being acquisition and visualization of incoming measurement data, control of the processing/production, and data storage [13]. Such systems were not originally designed to handle cyberattacks, and thus can be an attractive targets. Potential vulnerabilities in this regard (due to the human and other factors) include: using (default) usernames and passwords, unencrypted communication, weak credential management, weak authentication, and ineffective threat planning/mitigation processes [14]. The risk is made even more palpable by the fact that energy generators (including self-consumers) are increasingly using SCADA systems on personal equipment such as mobile phones (smartphones) or tablets, which are dual-use (private and business) devices. This exacerbates the risk of a third party gaining unauthorized access to a SCADA system (a generation unit or transformer station) and thus potentially taking over the basic control functions for the

unit [12]. One such attack targeted the Ukrainian energy system in 2015, specifically the Ukrainian distribution company Kyivoblenergo. The attackers sent e-mails to the company employees containing infected Word and Excel. Opening the files caused BlackEnergy3 RAT (Remote Access Tools) malware to install itself on the workstations (computers) and enable remote access to Internet-connected workstations. The attackers gained access to the power company's SCADA, leading to seven 110 kV grids and twenty three 35 kV grids becoming disconnected, leaving approx. 225,000 customers without power, including the regional capital of Ivano-Frankivsk [15,16].

Whether a unit is connected to the internet or not, one should not underestimate the risks of infection with viruses, worms or Trojan horses (which facilitate infiltration and takeover), including those stored on external media. One such incident occurred in 2016 when the Gundremmingen (Germany) atomic plant control system was found to have been infected with "W32.Ramnit" and "Conficker" viruses. The viruses were probably injected into the system during a 2008 upgrade. The malware was found in data visualization software associated with equipment for moving nuclear fuel rods, as well as computer disks and USB sticks. The infection did not disrupt the operation of the plant itself or any other power company (such as grid operators), because the infected components were not connected to the Internet [17].

With regard to cross-border energy trade, it is important to consider that the lack of suitable coordination procedures can also lead to potential incidents and cyber threats to the operation of transmission/distribution grids. For example, in 2013, a misconfiguration in the control system of the Austrian electricity transmission grid operator led to near-total loss of ability to supply energy to customers. The incident was sparked by a status request command packet sent by a German gas company to check the status of their newly commissioned gas network. However, the query was also accidently (erroneously) received by the Austrian energy power control and monitoring network, which led to the generation of thousands of reply messages in the power system, which then generated even more data packages, eventually overloading the system and cutting off services. The incident was caused by a misinterpretation of the data signal at an interface of two domains from two different energy sub-sectors. As a result, the relevant energy system functions were unavailable for a time [12]. The incident, though not intentional, is classified as a DDoS attack (distributed denial of service)—an attack on a computer system or network service intended to render it inoperable by draining all available resources. In this particular case, the effects could only be neutralized by isolating part of the monitoring & control network and disconnecting it from the internet. Although this incident did not cause any power outages, it does speak to the cross-border impact of threats and the interdependencies between energy sub-sectors.

4. Towards a Normative Framework for Cybersecurity in the Energy Sector

4.1. Horizontal Regulations

One of the first EU documents that comprehensively dealt with the issue of cybersecurity (within the framework of the New Approach) was the aforementioned 2013 Cybersecurity Strategy of the European Union. The Strategy highlighted the need to strengthen EU cybersecurity resilience by engaging not only public authorities, but the private sector as well. However, it bears mentioning that it was not the EU's first action that tackled network and information security. As early as 2001, the Commission adopted a Communication on "Network and Information Security: Proposal for a European Policy Approach" (COM (2001) 298). Similarly, in 2004, Regulation 460/2004/EC of the European Parliament and of the Council (Official Journal EU of 19 March 2004, L 77/1) established the European Network and Information Security Agency (ENISA) to provide assistance and deliver advice to the Commission and the Member States on issues related to network and information security (including preparatory work for updating and developing EU legislation in the field of network and information security), as well as maintain expertise to stimulate cooperation between actors from the public and private sectors. Later, in

2006, the Commission adopted a "Strategy for a Secure Information Society—Dialogue, partnership and empowerment" (COM(2006) 251 final). Finally, in 2009, the EC published a Communication titled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM (2009) 149 final). In line with the European Programme for Critical Infrastructure Protection (EPCIP), the Communication called for strengthening the security and resilience of critical infrastructures, especially ICT infrastructures—thus fully realizing the economic and social opportunities of the information society. The EC strongly stressed the need for actors to coordinate their actions so that cross-border cyber threats be managed more successfully. Crucially, the document delineated strategic priorities for neutralizing cyberspace-originating threats. The most important of these are: achieving cyber resilience; drastically reducing cybercrime; developing cyberdefense policy and capabilities related to the framework of the Common Security and Defense Policy (CSDP); developing industrial and technological resources for cybersecurity; and establishing a coherent international cyberspace policy for the European Union. The EC also noted that despite the progress made based on voluntary commitments, normative regulation of cybersecurity was still needed. Therefore, the strategy was accompanied by a proposal for legislation to:

- establish common minimum requirements for network and information security at national level;
- establish coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities;
- improve preparedness and engagement of the private sector, due to the fact that a large majority of network and information systems are privately owned and operated.

As a result of the above, 2016 saw the adoption of a follow-up Directive concerning measures for a high common level of security of network and information systems across the Union (also known as the NIS Directive, from "network and information systems") [18]. The ratio legis behind this legislation is to respond effectively to the challenges of the security of network and information systems at Union level, covering common minimum capacity building and planning requirements, exchange of information, cooperation, and common security requirements for operators of essential services and digital service providers. For this purpose, the Union legislator requires Member States to adopt national strategies on:

- the security of network and information systems, defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems;
- creating a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States, to develop trust and confidence amongst them, to create a Computer Security Incident Response Team (CSIRT) to contribute to the development of trust and confidence between Member States, and to promote swift and effective operational cooperation;
- establishing security and notification requirements for operators of essential services and for digital service providers;
- laying down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems (Article 1 (2) of the NIS Directive).

One of the key features of this act is the definition of "operators of essential services". The criteria used to define them are similar to those for classifying an entity as essential under the Proposal for a Directive on resilience of critical entities (RCE Proposal). In both cases the entities are those which are considered to provide essential services dependent on a specific infrastructure (in this case—network and information systems), services which would be significantly disrupted if the entity were to fall victim to an incident. Of key importance is the difference between service provision and an actual infrastructure. According to the proposed RCE Directive, this infrastructure consists of assets, a system or part

thereof. The NIS Directive instead focuses on network and information systems, including electronic communications networks, any devices or groups of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of digital data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection or maintenance. Consequently, it should be assumed that the "infrastructure" referred to in the proposed RCE Directive is preponderant over the "information networks and systems" mentioned in the NIS Directive. This is because networks and information systems are intended to provide certain services, e.g., electricity or natural gas, using dedicated "infrastructure" (e.g., transmission or distribution grids). What is crucial is that digitization has made it impossible in many cases to provide such services without the above-mentioned assets. In practice, this means that the designated "critical entities" may also qualify as operators of essential services. However, these two categories should not be automatically considered to be equivalent. After all, it must be borne in mind that the proposed RCE Directive covers a wider set of sectors and subsectors than the NIS Directive (10 versus 7 sectors). The energy sector alone, which includes the electricity, gas and oil subsectors, is expanded to include heating, cooling and hydrogen systems.

Consequently, an entity may be designated as critical without necessarily being recognized as an operator of essential services. Moreover, the NIS Directive does not specify that cross-border elements are a required qualifier for a significant disruptive effect (Table 1). Nevertheless, while this criterion is not required for an entity to be designated as critical, it does determine whether it is classified as a critical entity of particular European significance. The proposed RCE Directive cites the geographic area that could be affected by an incident, including any cross-border impacts, as one of the prerequisites for the significance of an disruptive effect (Article 6 (1) (e) of the proposed RCE Directive). Essential services on the other hand are defined as those which are provided to or in more than one third of Member States (Article 14 (2) of the proposed RCE Directive). This distinction is important due to the different obligations (including supervision) and powers the two statuses bestow. The NIS Directive also seems to focus on the Member States and the cooperation between them within the so-called "Cooperation Group" (which also includes the Commission and ENISA) or the CSIRT network (consisting of representatives of the Member States and the CERT-EU—Computer Emergency Response Team), whereas the proposed RCE Directive is more concerned with entities providing essential services, including their obligations and supervision. These include: giving strategic advice on the operation of the established CSIRT network; exchanging best practice on sharing incident reporting information; discussing the capacity and readiness of Member States; and (on a voluntary basis) evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, exchanging information and best practice on awareness-raising and training (Article 11 (3) of Directive 2016/1148/EU). In many cases, the provisions of these acts do overlap to some extent. One example is the requirement placed upon Member States to develop a "Strategy on the resilience of critical entities" and a "National strategy on the security of network and information systems", along with the other aforementioned provisions (disruptive effect, incident reporting, risk assessments, etc.). This may raise question as to the consistency of both acts and confusion with regard to excessive regulation. However, in this regard, it bears noting that the proposed RCE Directive should be interpreted in conjunction with the proposed amendment to the NIS Directive, tabled by the EC in December 2020 (known as the NIS 2 Directive). Both acts fall into the updated EC cybersecurity strategy aimed at strengthening the Union's strategic autonomy (to improve its resilience and collective response and to build an open and global Internet) [19] and increasing interconnection and interdependency between physical and digital infrastructures. At the same time, given the importance of cyber security to resilience of critical entities, these legal acts will complement each other in practice. This is particularly important, since keeping the 2016 NIS Directive in its current form could lead to excessive burden on entities providing essential services and ineffectiveness of the

adopted legislation. It should be noted that the strategy is an extension of the Common Position (2017) of the EC and the High Representative of the Union for Foreign Affairs and Security Policy on cybersecurity, which calls for strengthening ENISA by granting the agency a permanent mandate, as well as building a single cybersecurity market, which would include:

- setting up an EU cybersecurity certification framework, fully implementing the Directive on the Security of Network and Information Systems and the associated changes,
- improving resilience through rapid emergency response,
- enhancing EU cybersecurity capabilities by forming cybersecurity competence networks with the European Cybersecurity Research and Competence Centre,
- building a strong EU cyber skills base, promoting cyber hygiene and awareness,
- identifying malicious actors,
- stepping up the law enforcement response,
- public-private partnership on combating cybercrime,
- stepping up the political response,
- building cybersecurity deterrence through the Member States' defense capability,
- promoting cybersecurity in external relations, building cybersecurity capacity, and EU-NATO cooperation [20].

Table 1. The list of sectors, subsectors and types of entities in the NIS directive and the proposal of NIS 2/RCE Directives.

NIS Directive	Proposal of NIS 2/RCE Directive
Energy **(a) Electricity** - Electricity undertakings which carry out the function of 'supply' - Distribution system operators - Transmission system operators **(b) Oil** - Operators of oil transmission pipelines - Operators of oil production, refining and treatment facilities, storage and transmission **(c) Gas** - Supply undertakings - Distribution system operators - Transmission system operators - Storage system operators - LNG system operators - Natural gas undertakings - Operators of natural gas refining and treatment facilities	**Energy** **(a) Electricity** - Electricity undertakings which carry out the function of 'supply' - Distribution system operators - Transmission system operators - Producers - Nominated electricity market operators, - Electricity market participants **(b) District heating and cooling** - District heating or district cooling **(c) Oil** - Operators of oil transmission pipelines - Operators of oil production, refining and treatment facilities, storage and transmission - Central oil stockholding entities **(d) Gas** - Supply undertakings - Distribution system operators - Transmission system operators - Storage system operators - LNG system operators - Natural gas undertakings - Operators of natural gas refining and treatment facilities **(e) Hydrogen** - Operators of hydrogen production, storage and transmission

Source: Own study based on the NIS Directive and the proposal of NIS 2/RCE Directives.

In addition to the considerations described above, another impetus to introduce the new legislation came in the form of a periodic evaluation by the EC, pursuant to Article 23 of the NIS Directive, which identified a number of persisting problems, especially: low level of cyber resilience of businesses operating in the EU, inconsistent resilience across Member States and sectors, the level of joint situational awareness, and lack of a joint crisis

response. An amendment of the NIS Directive has become even more pressing since the onset of the COVID-19 crisis, which further amplified the listed problems.

As was the case in the proposed RCE Directive, the list of energy subsectors was expanded to include heating, cooling, and hydrogen systems. Such an approach appears to be justified, given the prominence of these sectors in the new EU energy policy. As a result, the entities indicated in the Annexes to these proposals have been assigned a dual role—that of critical entities and essential entities. This is not universal, however, since the proposed RCE Directive requires not only that an entity belong to one of the subsectors listed in the Annex to the proposal—it must also meet the prerequisites indicated in Article 5 (2) of the proposed RCE Directive. In the context of the proposed NIS 2 Directive, the second category is a novel provision absent from existing regulations, which state that "operators of essential services" are identified by Member States via a two-step procedure. This process required additional financial and human resources and thus proved overly complicated, leading to highly varying success in identifying such entities [19]. As a result, there has been a widening cybersecurity gap between different Member States. The proposed Directive tackles this issue and simplifies the system by introducing a category of "essential and important entities", which will be legally required to meet the standards of the NIS 2 Directive, assuming that they are included in the sectors listed in Annex 1 to the draft. In general, the risk management and incident reporting requirements are similar to the original ones. On the other hand, to strike a fair balance, changes have been made to the supervision and penalty regime. For example, the electricity sector encompasses: electricity undertakings which carry out the function of "supply", distribution system operators, transmission system operators, producers, nominated electricity market operators, electricity market participants providing aggregation, demand response or energy storage services. Entities included in this category have been obliged to take appropriate technical and organizational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. (Article 18 (2) of the proposed NIS 2 Directive). The major requirements include:

- risk analysis and information system security policies,
- incident handling,
- business continuity and crisis management,
- supply chain security,
- security in network and information systems acquisition, development and maintenance,
- policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures, and
- the use of cryptography and encryption (Article 18 (2) of the proposed NIS 2 Directive).

Furthermore, the proposal introduces a higher level of harmonization of security and reporting obligations compared with the regulations correctly in place. This change will lessen the compliance burden, especially for entities providing cross-border services. Notably, the proposal also puts more stringent risk management requirements on companies classified as essential or important (in comparison to digital service providers/operators of essential services under the NIS Directive). It replaces the existing closed list of technical and organizational measures with a minimum list of elements which must be incorporated into risk management processes for network and information system security. The Union legislator has expanded this list of elements to include, among others: risk analysis and information system security policies; crisis management; security in network and information systems acquisition, development and maintenance; policies and procedures to assess the effectiveness of cybersecurity risk management measures; the use of cryptography and encryption; and supply chain security (Article 18 (2) of the proposed NIS 2 Directive). This last element is of particular importance for strengthening cyber security in ICT. The Member States, in cooperation with the Commission and ENISA, are to carry out coordinated security risk assessments of critical supply chains, using the proven approach with regard to the recommendation of the Commission on cybersecurity of 5G networks (Article 19 of the proposed NIS 2 Directive). The proposal also lays down stricter rules for incident

reporting and, crucially, imposes a 24 h time limit on essential/important entities for notifying incidents (after having become aware of the incident) to the competent authorities of the Member States or the CSIRTs (Article 20 (4) of the proposed NIS 2 Directive). According to Article 20 (4) of the proposed NIS 2 Directive, Member States must provide that in duly justified cases—and in agreement with the competent authorities or the CSIRTs—the entity concerned can deviate from the 24-h deadline for incident notification. The national authorities or the CSIRTs must provide, within 24 h after receiving the notification, "a response to the notifying entity, including initial feedback on the incident and, upon request of the entity, guidance on the implementation of possible mitigation measures" (Article 20 (5) of the proposed NIS 2 Directive,). The CSIRT provides additional technical support if the concerned entity so requests. Where the incident is suspected to be of criminal nature, the competent national authorities or the CSIRTs also provide guidance on reporting the incident to law enforcement authorities (Article 20 (5) of the proposed NIS 2 Directive). Presumably, this particular regulation is aimed at ensuring a more effective response to threats and reducing potential negative consequences of incidents. An important (new) element introduced to improve the information exchange system (and, consequently, responsiveness to incidents) is the provision obliging essential and important entities to notify the recipients of their services of incidents that are likely to adversely affect the provision of that service (Article 20 (5) of the proposed NIS 2 Directive). This regulation is supplemented by another obligation, stating that essential and important entities must provide any information enabling the competent authorities or the CSIRTs to determine any cross-border impact of the incident. This requirement should be applied in conjunction with the regulation set out in Article 20 (6), which states that if the incident concerns two or more Member States, the competent authority or the CSIRT must inform the other affected Member States and ENISA of the incident. In the energy sector, such a situation may arise if an incident affects an infrastructure used by transmission (or distribution) system operators via interconnectivity. This may prove particularly important for short-term markets (DAM and IDM, where the transaction occurs within the timeframe of two days to one hour prior to the delivery of electricity) because it necessitates an immediate reaction to neutralize the source of the incident in order to ensure continuity of supply. It also appears that the regulation will be important for balancing markets, where the electricity demand is matched to generation in real time. On a cross-border level, an incident that disrupts the operation of nominated electricity market operators (NEMOs) could reasonably affect two or more Member States. After all, these entities by definition perform the function of a market coupling operator by matching and executing orders for purchase/sale of electricity for the DAM and the IDM (under the SDAC and SIDIC/XBID projects), while simultaneously allocating cross-border capacity for different market areas. Thus, for example, an incident disrupting the authenticity of the data processed by a NEMO on the orders transmitted to a TSO could hinder (distort) effective allocation of cross-border capacity at congestion points.

When notifying an incident, essential and important entities should also indicate whether the incident is caused by unlawful or malicious action. However, this obligation is not absolute—the Union legislator made its applicability conditional upon the existence of an unlawful or malicious action to the best knowledge of such essential and important entities (the working used is "presumably") on the potential causes of the incident. However, in authors' opinion the discussed provision may prove ineffective, regardless of the nature of the regulation. First of all, it must be recognized that essential and important entities often lack the adequate technical, human or financial resources to identify the source of an incident. The multilateral nature of cyberattacks makes it extremely difficult to determine (even on a "presumed" basis) whether the incident is caused by unlawful or malicious action within 24 h. As a consequence, depending on the practice prevalent in the given country, entities may end up reporting each and every one of such "presumptions"—even if they have no basis in reality, but are notified simply as a precaution to avoid potential liability for non-compliance with applicable law. Perhaps this issue can be resolved when

the Directive is implemented in the national legal systems. However, if so, this could again lead to a situation where the burdens imposed on essential and important entities differ from one Member State to another. This, in turn, may delay the process of identifying the real source of an incident by law enforcement—though even such identification does not ensure that the perpetrator will be brought to justice.

Another important element of the new cybersecurity framework is the permanent mandate granted to ENISA (the previous mandate expired in 2020). This provision is intended to achieve a high common level of cybersecurity, including by having ENISA provide active support to Member States, Union institutions, bodies, offices, and agencies in improving cybersecurity. This mandate is granted under Article 3 of Regulation 2019/881/EU (also known as the Cybersecurity Act), which establishes institutional framework on cybersecurity and unified ICT certification. As set out in Article 1 (1) of Regulation 2019/881/EU: "With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down: (a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union." One provision, important for cross-border trading, calls for a certification system to verify that ICT products, ICT services, and ICT processes conform to unified requirements regarding the protection of accessibility, authenticity, integrity and confidentially of stored, transmitted or processed data or of the related functions or services offered by, or accessible via those products, services and processes throughout their life cycle (see Articles 48 to 58 of Regulation 2019/881/EU). This system relieves entities from the need to go through several certification processes when trading across borders, thereby limiting administrative and financial costs and improving the resilience of the energy system.

One particularly important provision of the NIS 2 Directive is the creation of a registry for essential/important entities and cross-border service providers (including identification data), to be maintained by ENISA (Article 25 of the proposed NIS 2 Directive). Notably, this regulation will oblige ENISA to send the data of essential and important entities to "single points of contact". According to Article 8 (3): "Each Member State shall designate a national single point of contact on the security of network and information systems ("single point of contact"). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State." The significance of these points lies in their function as liaisons to ensure cross–border cooperation of a Member State's authorities with the relevant authorities in other Member States, as well as to ensure cross-sectorial cooperation with other national competent authorities within the Member State (Article 8 (4) of the proposed NIS 2 Directive). Furthermore, the proposal expands ENISA competences to include: developing and maintaining a European vulnerability registry (Article 6 (2) of the proposed NIS 2 Directive), preparing an annual report on the state of cybersecurity in the Union (Article 15 of the proposed NIS 2 Directive) and collecting aggregated incident data from Member States and issuing technical guidance (Article 20 (9) of the proposed NIS 2 Directive). The cooperation was broadened to include mutual assistance between Member States referred to in Article 34 of the proposed NIS 2 Directive. The registry is to include, in particular: information on the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. The act requires ENISA to cooperate with Member States and other authorities: those already in place under the existing NIS Directive—i.e., Cooperation Groups and CSIRTs—and the newly established—the European cyber crises liaison organization network (EU—

CyCLONe). It also provides an interesting and relevant tool in the form of the peer-review of Member States' cybersecurity policies, performed on the basis on the methodology established by the EC following consultation with the Cooperation Group and ENISA. The reviews are to be conducted by cybersecurity technical experts drawn from Member States different than the one reviewed (Article 16 of the proposed NIS 2 Directive). Such a system would seem to promote the harmonization of cyber security levels across the Member States. From a practical point of view this solution will enable a more objective assessment of the state of cyber security in a particular Member State and identification of areas requiring further improvement. However, the question remains open as to the extent to which the Member States will actually incorporate the assessment into their strategies, since the proposal does not include any provisions that would oblige them to do so. The only requirement in this regard calls for reports on the assessment of cybersecurity policy effectiveness, to be submitted to the Commission, the Cooperation Group, the CSIRTs network and ENISA, and discussed in the Cooperation Group and the CSIRTs network (Article 6 (7) of the proposed NIS 2 Directive).

4.2. Sector-Specific Regulation as a Complement to Cybersecurity Strategies in the Energy Sector

While previous legislature was horizontal in nature, the EU has also recognized the need to introduce individualized, sector-specific regulations on cyber security. This is primarily dictated by the unique nature of individual sectors. In the case of the energy sector, this specificity stems from the combination of old and new information technologies, particularly with the real-time requirements of the power grid.

The need to introduce sector-specific cybersecurity regulations in the energy sector was even more strongly emphasized in the package "Clean energy for all Europeans". Digital transformation in the energy sector is one part of the EU strategy to achieve the objectives of its new low-carbon policy. The 2019 EC Recommendation on cybersecurity in the energy sector is a key document on this issue [21,22]. Though not legally binding, the Recommendation set out a framework for Member States, energy grid operators, and digital providers on issues related to cybersecurity in the energy sector (real-time requirements, cascading effects, and combination of legacy and state-of-the-art technology) and the main actions for implementing relevant cybersecurity preparedness measures in the sector. Since elements of the energy system need to work under "real time" (react to commands within a few milliseconds) and combine new technology with old, the main recommendations of the EC were to:

- apply the most recent security standards for new installations (e.g., IEC, ISO, CEN);
- implement international standards on cybersecurity and adequate specific technical standards for secure real-time communication;
- consider real-time constraints;
- split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures;
- implement suitable cybersecurity readiness measures with regard to combinations of legacy and state-of-the-art technology in the energy sector;
- ensure that new devices, including Internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality;
- consider cyber-physical effects when establishing and periodically reviewing business continuity plans;
- establish design criteria and an architecture for a resilient grid;
- analyze the risks of connecting legacy and Internet of Things concepts and be aware of internal and external interfaces and their vulnerabilities;
- take suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications;
- establish an automated monitoring and analysis capability for security-related events.

These recommendations are mostly targeted at operators of essential services. For the energy sector, these operators include transmission and distribution system operators,

electricity suppliers, and gas suppliers. When the NIS 2 Directive enters into force, these standards should be extended to essential and important entities, for obvious reasons. Of note for cross-border trade and investment is Commission's statement that energy operators need to evaluate the interdependencies and criticality of power generation and flexible-demand systems, transmission and distribution substations and lines, and the associated entities impacted by cross-border effects of a successful cyber-attack or cyber incident. This approach is consistent with the existing regulatory framework (the NIS Directive and the ENISA Regulation), as well as proposals for new legislation (RCE and NIS 2 Directives).

The sector-specific regulations are supplemented by Directive 2019/941/EU on risk-preparedness in the electricity sector and repealing [23]. Although the regulation does not directly regulate the cybersecurity, it does recognize cyberattacks (in addition to other sources, such as extreme weather conditions) as a potential source of power outages (Recital 2 of Regulation 2019/941/EU). Even if markets and systems function well and are interconnected. Consequently, recognizing that the effects of electricity crises often extend beyond national borders, this act's primary focus is in unifying the rules of prevention and crisis management in the electricity sector. To that end, it provides for common:

- methods for the assessment of risks to security of electricity supply (Articles 4 to 9 of Regulation 2019/941/EU),
- rules and framework for crisis management, and
- assessment and monitoring of electricity supply security (Articles 17 and 18 of Regulation 2019/941/EU).

A similar legal act (in terms of securing uninterrupted supply of energy, in this case of natural gas, throughout the Union) is Regulation 2017/1938/EU concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 [24]. Similar to Regulation 2019/941/EU, this act provides for mechanisms concerning the coordination of planning for, and response to, emergencies at national, regional, and Union level, in order to prevent disruption to the continuity of natural gas supply to individual Member States and the EU, as well as implement appropriate mitigation measures if a disruption does occur. The Regulation places the joint responsibility for the security of gas supply on natural gas undertakings, Member States, and—where appropriate—the Commission itself. A Gas Coordination Group (GCG) is established under the Regulation to facilitate the coordination of measures concerning the security of gas supply. The GCG is composed of representatives of the Member States, in particular representatives of their competent authorities, as well as the Agency for the Cooperation of Energy Regulators, ENTSOG and representative bodies of the gas industry and those of relevant customers (Article 4 (1) of Regulation 2017/1938/EU). The Union legislator stresses the need for solidarity between Member States, including by providing (on a solidarity basis) natural gas to customers in another Member State in the event of an emergency (Article 13 of Regulation 2017/1938/EU). As far as cybersecurity is concerned, the Regulation cites cyberattacks and ICT failure (hardware or software failure, Internet, SCADA problems, etc.) as a technological risk factor that must be included in a common risk assessment prepared by a given risk group (encompassing selected Member States, depending on the route of gas supply). The scope of this act also seems to be somewhat broader than that of Regulation 2019/941/EU. It sets out unified standards regarding gas infrastructure and supply, which makes it somewhat similar to technical regulations under network codes (Articles 5 and 6 of Regulation 2017/1938/EU). For example, in the event of a disruption of the single largest gas infrastructure, the technical capacity of the remaining infrastructure (determined in accordance with the N—1 formula as set out in point 2 of Annex II) should be able to satisfy total gas demand of the calculated area during a day of exceptionally high gas demand occurring with a statistical probability of once in 20 years (Article 5 (1) of Regulation 2017/1938/EU). Nevertheless, there are no equivalent (technical) provisions in the Regulation which would explicitly refer to cyber security in the gas sector. It would seem prudent to regulate this matter in future network codes or gas guidelines. However,

the current legal framework offers no explicit legal basis for the adoption of a network code on cyber security of cross-border natural gas flows by the EC. Presumably, due to the vital importance of the issue, relevant regulations will be adopted in the new cross-border gas regulation. This is supported by the fact that appropriate delegating provisions are included in the new electricity regulation, which authorizes the EC to adopt technical rules for cybersecurity aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting, and crisis management (Article 59 (2) (e) of Regulation 2019/943/EU).

5. Conclusions

The need to ensure cybersecurity in the energy sector has definitely become more pressing in recent years. In fact, the same is true for other sectors of the economy. A telling example of the fast-progressing changes (further intensified by the COVID pandemic) is the proposed NIS 2 Directive, put forward no more than 5 years after the adoption of the original NIS. Whereas the regulation introduced in the 2000s was primarily focused on the physical protection of critical infrastructure, this focus has clearly shifted to countering cyber threats, and it is plainly obvious that this shift was spurred by the recent technological advances. It would also be reasonable to posit that the security of electricity and natural gas supply is a broader concept than years ago. Due to the progressing digitalization of the energy sector, and the inter- and intra-sectoral and cross-border interdependencies, security is impossible to enforce without suitable cybersecurity regulation in this specific area. Even a few years ago, cybersecurity was not usually associated with the security of gas/electricity supply. The functioning of the single energy market, as well as free energy trade and investment, also draw similar connotations.

Although the regulations adopted to date have been horizontal in nature, it appears that they may prove insufficient for the purposes of EU energy market integration. However, the code on cybersecurity aspects of cross-border electricity flows marks a return to a sector-specific approach to energy infrastructure protection, at least to some extent. In particular, the issue of cross-border risk assessment and management of cyber threats in the energy sector requires dedicated regulation. Although this area has been subject to partial regulation, it has mostly concerned TSOs (as an operator of key services) and cross-border effects, placing less focus on appropriate standards of conduct and cooperation between specific entities (e.g., TSOs and DSOs) to counteract (and manage) cross-system cyber threats. This is despite the fact that both TSOs and DSOs (and other entities, such as electricity generators) belong to specific regional synchronous areas. A disruption of one such area due to a cyber attack or cyber incident can therefore affect the operation of the entire synchronous area.

Finally, it is well worth noting the proposal for the NIS 2 Directive. I would assess the initiative as a whole as a positive development. Though the submission of a completely new regulation in such a short period of time after the adoption of the original piece of legislation may give rise to some confusion, this can only be interpreted as a manifestation of the ever-faster changes in the sphere of cyber security (in part due to the COVID-19 pandemic). By way of contrast, in the case of the ECI Directive, the legislator decided against changing its provisions (justifying this, inter alia, by the high costs of implementing the new provisions), despite a negative evaluation. The full effectiveness of the regulation discussed in the present paper will be determined by the final network code on cyber security in cross-border energy flows. At the same time, given the unpredictability intrinsic to new technologies, it seems likely that the regulations in this area will need to be periodically amended.

Funding: University of Warmia & Mazury, Faculty of Law & Administration.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Gajewski, J.; Paprocki, W.; Pieriegud, J. *Cyfryzacja Gospodarki i Społeczeństwa—Szanse i Wyzwania dla Sektorów Infrastrukturalnych*; Gdańsk, Instytut Badań nad Gospodarką Rynkową–Gdańska Akademia Bankowa: Katowice, Poland, 2016; p. 12.
2. Gobble, M.M. Digitalization, Digitization, and Innovation. *Res.-Technol. Manag.* **2018**, *61*, 56–59. [CrossRef]
3. Di Silvestre, M.L.; Favuzza, S.; Sanseverino, E.R.; Zizzo, G. How Decarbonization, Digitalization and Decentralization are changing key power infrastructures. *Renew. Sustain. Energy Rev.* **2018**, *93*, 483–486. [CrossRef]
4. Anwar, A.; Mahmood, A. Cyber security of smart grid infrastructure. In *The State of the Art in Intrusion Prevention and Detection*; Pathan, A.K., Ed.; CRC Press, Taylor & Francis Group: New York, NY, USA, 2014; pp. 449–472.
5. Singh, N.; Mahajan, V. End-User Privacy Protection Scheme from Cyber Intrusion in Smart Grid Advanced Metering Infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100410. [CrossRef]
6. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. *Comput. Netw.* **2020**, *169*, 1–13. [CrossRef]
7. ENISA Overview of Cybersecurity and Related Terminology. Version 1. September 2017. p. 6. Available online: https://www.enisa.europa.eu (accessed on 3 May 2021).
8. Recital 5 of 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) OJ L 151/15, 7 June 2019. Available online: https://eur-lex.europa.eu/ (accessed on 1 September 2021).
9. European Commission. High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 Final, s. 2. Available online: https://eur-lex.europa.eu/ (accessed on 10 September 2021).
10. European Commission. High Representative of the Union for Foreign Affairs Security Policy, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, JOIN(2017) 450 Final. Available online: https://eur-lex.europa.eu/ (accessed on 15 September 2021).
11. Warchoł, A. Pojęcie Cyberprzestrzeni w Strategiach Bezpieczeństwa Państw Członkowskich Unii Europejskiej, Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate 2019, No 9 (4). Available online: https://eur-lex.europa.eu/ (accessed on 30 September 2021).
12. Fischer, L.; Uslar, M.; Morrill, D.; Döring, M.; Haesen, E. *Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector*; European Commission: Berlin, Germany, 2018; EC Reference: ENER/B3/2017-465.
13. Kermani, M.; Adelmanesh, B.; Shirdare, E.; Sima, C.A.; Carnì, D.L.; Martirano, L. Intelligent Energy Management Based on SCADA System in a Real Microgrid for Smart Building Applications. *Renew. Energy* **2021**, *171*, 1115–1127. [CrossRef]
14. Malko, J.; Wojciechowski, H. "Nowa Energia" 2015, No 1. Available online: https://www.cire.pl/pliki/2/sektorenbezpcyb.pdf (accessed on 22 May 2021).
15. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 10. [CrossRef]
16. European Parliament. Cybersecurity of Critical Energy Infrastructure. Available online: https://www.europarl.europa.eu (accessed on 22 May 2021).
17. Bisson, D. 3 ICS Security Incidents that Rocked 2016 and What We Should Learn from Them. Available online: https://www.tripwire.com/state-of-security/ics-security/3-ics-security-incidents-rocked-2016-learn/ (accessed on 22 May 2021).
18. Germany's Gundremmingen Power Plant Hit by Computer Viruses. Available online: https://laptrinhx.com/15ermany-s-gundremmingen-power-plant-hit-by-computer-viruses-3681491308/ (accessed on 19 May 2021).
19. 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, OJ L 194/1, 19 July 2016. Available online: https://eur-lex.europa.eu/ (accessed on 1 October 2021).
20. European Commission. Proposal. 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, pp. 1–2. Available online: https://eur-lex.europa.eu/ (accessed on 5 October 2021).
21. Commission Recommendation (EU) 2019/553 of 3 April 2019 on Cybersecurity in the Energy Sector, C (2019) 2400, OJ L 96/50, 5 April 2019. Available online: https://eur-lex.europa.eu/ (accessed on 20 October 2021).
22. Witkowska, A. Cybersecurity Challenges in Poland it the Face of Energy Transition. *Yearb. Inst. East-Cent. Eur.* **2020**, *18*, 147–148.
23. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC, OJ L 158/1, 14.6.2019. Available online: https://eur-lex.europa.eu/ (accessed on 14 October 2021).
24. Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 Concerning Measures to Safeguard the Security of Gas Supply and Repealing Regulation (EU) No 994/2010, OJ L 280/1, 28 October 2017. Available online: https://eur-lex.europa.eu/ (accessed on 20 October 2021).