



Overview and Improvement of Procedures and Practices of **Electricity Transmission System Operators in South East Europe** to Mitigate Cybersecurity Threats

Aleksandra Krkoleva Mateska 1,* , Petar Krstevski 1 and Stefan Borozan 1,2

- Faculty of Electrical Engineering and Information Technologies, Ss Cyril and Methodius University in Skopje, 1000 Skopje, North Macedonia; petark@feit.ukim.edu.mk (P.K.); stefanb@pees-feit.edu.mk (S.B.)
- Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, UK
- Correspondence: krkoleva@feit.ukim.edu.mk

Abstract: The implementation of information and communication technologies (ICT) in power systems increases the risks of cybersecurity threats, requiring protection measures that should reflect the multi-actor environment of the contemporary power systems. This paper provides a critical assessment of the cybersecurity practices of the transmission system operators (TSOs) from South East Europe (SEE) and the implementation of obligations for TSOs emerging from the complex set of cybersecurity and electricity legislation. The analyses of TSO cybersecurity practices are based on a survey conducted with the TSOs from SEE and show there is a lack of consistent cybersecurity policy at the TSO level. These analyses demonstrate that the differences between TSOs from the SEE region are not very significant with regards to implementation of technical protection and defense measures for critical infrastructures (CIs) and assets. The comprehensive analyses of electricity and cybersecurity legislation uncover the obligations of TSOs emerging from legislation and relate them to current TSO cybersecurity practices, confirming the necessity to boost existing practices. Considering the analyzed legislation and implemented practices, this paper presents a proposal for a cybersecurity framework for TSOs that should improve their organizational and operational response to the evolving cybersecurity challenges.

https://doi.org/10.3390/systems9020039 Keywords: transmission systems; cybersecurity; critical infrastructure



Citation: Krkoleva Mateska, A.; Krstevski, P.; Borozan, S. Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats, Systems 2021, 9, 39.

Academic Editors: Rodney Stewart and Oz Sahin

Received: 9 May 2021 Accepted: 27 May 2021 Published: 2 June 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).

1. Introduction

Power systems have changed significantly over the past thirty years. These changes resulted from the need to optimize power systems operation, the need to enable electricity trade and develop transparent electricity markets for all stakeholders, and the need to diversify the electricity production and increase the use of clean energies. Therefore, higher requirements on security of operation, reliability and flexibility of power systems are set, demanding additional changes in power systems architecture, their operation and control. As a result, the use of industry control systems (ICS) and penetration of new ICT has significantly increased [1]. The implementation of advanced control techniques based on ICT as well as the extensive use of ICS are the cornerstones of the evolution of contemporary power systems into cyber-physical power systems (CPPSs). A CPPS consists of a physical system (equipment) which is integrated with control, computing and communication functions and enables both flow of electricity and information [2]. Thus, CPPSs are facilitating the shift towards the Smart Grids paradigm and the penetration of its technologies. During this ongoing transformation process, electricity system operators have the responsibility to manage and operate simultaneously two different, but highly interdependent and complex infrastructures. The use of ICT significantly changes the operation of power systems, but it also introduces new threats to system assets and new

Systems **2021**, *9*, 39 2 of 21

challenges for the operation of transmission networks. Consequently, cybersecurity has become an important issue that has to be addressed by system operators.

The objective of this paper is to present the results of the investigation of current cybersecurity practices of the TSOs from eight countries in SEE and propose applicable measures and practices that will increase the cybersecurity of the information systems and ICS used in transmission networks. This paper proposes a new cybersecurity framework, in line with the latest European legislation, to be implemented on company level and to improve the cybersecurity practices of TSOs. The necessity for such a framework emerges from the analyses of the collected data and inputs from the TSOs in SEE, as well as from the investigation of the current legal framework and its future development. The inputs from the TSOs increase the relevance of the performed research and point to the shortcomings in their approach in dealing with cybersecurity threats. However, the role of TSOs in provision of the essential service of electricity transmission requires that the analyses consider both cybersecurity and electricity regulatory frameworks. Consequently, an extensive critical assessment of legislation has been performed to uncover the emerging obligations of TSOs and present them in a comprehensible manner. These findings have been combined with technical solutions used by TSOs to develop an applicable framework for increasing the cybersecurity at the TSO level. The work presented in this paper provides both in-depth and extensive analyses of all these issues, which has not been done in related work. The research presented in this paper builds on previous work of the authors presented in [1,3] and their research undertaken in [4].

1.1. Background on Cybersecurity Issues in Power Systems

Starting from the Slammer worm that infected the Davis-Besse nuclear power plant in Ohio in 2003 and affected its safety parameters display system [5], the number of cyberattacks on energy systems, including power systems, has increased [6]. These complex attacks were targeted and intended to sabotage the operation of energy utilities and cause disruption in their services. In the USA, [7], out of 290 cyber-incidents in 2016, 59 have been reported in the energy sector. Similarly, according to a study [8] of the European Union Agency for Cybersecurity (ENISA), the energy sector is among the three most impacted sectors with the highest incident associated costs. The problem becomes more complex for power systems, having in mind the combination in use of legacy and new technologies. This causes power systems to have functional equipment which was not designed for the fast-evolving cyber threats [9]. Furthermore, the ICS, including Supervisory Control and Data Acquisition (SCADA) systems, are becoming frequent targets for cyber-attacks [10], with 135 noted vulnerabilities in 2015, compared to 35 for the previous year. One of the first attacks on SCADA systems was recorded in 1982, when a malware introduced in the SCADA controlling a gas pipeline in Siberia caused an explosion that was equivalent to 3 tons of TNT [5]. The SCADA systems of factories, refineries and power plants are among the most frequently targeted, with global increase of SCADA attacks from 91,676 attacks in January 2012 to 675,186 attacks in January 2014 [11]. SCADA systems are the building blocks of Energy Management Systems (EMS) and are essential for remote control of equipment in the transmission systems substations, so attacks on these systems can cause large-scale effects on the operation and reliability of the power system, as discussed in [12]. A recent report encompassing the period from January 2019–April 2020 shows that the technology industry is among the top three targeted sectors [13], mostly through supply-chain attacks that compromise software development through backdoor attacks or zero-day exploits.

Successful cyber-attacks in power systems could have multi-fold effects. The disruption of the services of power companies is the most significant effect, followed by the potential impact on human wellbeing and financial implications of undelivered electricity, the potential equipment damage, and the possibilities for cascading effects and spread on neighboring transmission systems. Some of these effects, which have been observed in past attacks on power systems, are discussed in [6,14]. The rising sense of insecurity and

Systems **2021**, *9*, 39 3 of 21

panic is the underlying element of many cyber-attacks, but the effect of cyber-attacks on power systems is even greater as a huge number of people may be affected. For example, the attack in Ukraine in 2015 resulted in a power blackout in a part of the country and caused interruption of power supply to approximately 225,000 customers [15,16]. These events diminish the sense of trust and security in the systems and their capability to maintain continuous operation. The impacts of cyber-attacks on specific transmission system functions are considered in [17–19], i.e., the effects of cyber-attacks on state estimators are discussed in [17], the impacts on automatic generation control in [18] and load frequency control in [19]. The effects on data integrity attacks in electricity markets are studied in [20]. The specifics of cyber-attacks in distribution systems are studied in detail in [21] and a strategy for increasing the cyber security in distribution systems is proposed in [22].

These are the major reasons measures for protection and defense of power systems against cyber-attacks should be developed. The measures should ensure physical protection of CIs as well as protection of information infrastructure and networks from cyber threats. Bearing in mind the interactions of the physical and cyber segments of the CPPSs, cyber-attack estimation models for CPPS are developed and simulated in [23] and new security methodologies are developed in [24]. Various methods to increase the resilience of CPPSs are described in the review presented in [25] and state-of-the-art system security for CPPSs is reviewed in [26], showing the importance of analyses of threats and development of adequate testbeds for CPPSs. The CPPS interdependencies are also considered in [27] where solutions for eliminating the cascading effects of power systems on communication networks are developed. A more general approach, considering cyber physical systems [28] provides an extensive overview of the security vulnerabilities, threats and attacks, identification of key issues and challenges as well as analyses of the limitations of existing security measures applied in these systems.

1.2. Current Issues Related to Cybersecurity of TSOs in SEE

TSOs are responsible for the operation, security and maintenance of the transmission systems and therefore, have the responsibility to develop and implement measures and practices to ensure an adequate level of protection against cyber-attacks. As they are responsible for transmission of electricity, which is an essential service for the economy and society, their cybersecurity practices are also determined by the cybersecurity legislation framework, the intersectoral relations with other entities as well as by the specific obligations for security of their information and communication systems, i.e., the cyber domain of these CPPSs. In addition, the stipulations of various legislation should be incorporated in applicable company policies that should improve the cybersecurity of TSOs assets and information and communication infrastructure. The European Union (EU) has already introduced a number of acts [29–35] to improve the cybersecurity on EU and national level which also introduce obligations for TSOs, especially in terms of national and EU level cooperation.

The development of cyber protection systems is related to investments that have to be justifiable, thus requiring identification of CIs and deciding on the manner of their protection. This can be done following a risk-based approach by the TSOs [36] that considers the vulnerabilities of the critical assets and ICS and ensures a broad system analysis [37]. These measures should also include implementation of relevant standards as IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968 and IEEE 1815 (DNP3) [14]. Even in these cases, the stakeholders, i.e., the TSOs, should be prepared to find alternative and new ways to detect attacks in their systems by following novel approaches as described in [38]. Furthermore, on corporate level, the TSOs have to provide integration of various security measures into an applicable policy as well as to take into account threats that emerge on different operation levels and the possibility of coordinated attack scenarios [39].

While it is obvious that the topic of cybersecurity of transmission systems is becoming increasingly important and novel solutions for their protection and defense are being developed, the research presented in [14,40] shows that the TSOs in SEE should take

Systems **2021**, *9*, 39 4 of 21

considerable steps to organize a systematic approach in cyber threat mitigation. On one hand, their actions are bound by the available technical, financial and human resources, which may not be adequate to meet the requirements for increased cybersecurity nor for facing the challenge to manage the highly integrated physical and cyber domain in their systems. On the other hand, their role in provision of essential services and continuous evolution of cyber adversaries requires implementation of systematic actions and risk management.

Considering all these issues, this paper aims to cover the gap between the advanced research solutions for protection and defense of CPPSs and the current practices in place at the TSO company level, based on collected data from SEE countries. The implementation of the proposed measures and policy framework are essential to fill the gap between the cybersecurity requirements imposed by the evolving threats and the capabilities of the TSOs to face them. Taking a proactive and holistic approach, as presented in this paper, would enable the TSOs to act diligently against cyber threats at present and to implement more advanced solutions in the future.

2. Methods

2.1. Legislation

This paper provides a comprehensive overview of the complex set of electricity and cybersecurity legislation. The aim of the performed analyses is to uncover the obligations of TSOs emerging from legislation and relate them to current TSO cybersecurity practices. For this purpose, a top-down approach was used, starting with analyses of the obligations for TSOs emerging from EU legislation, national legislation, and cybersecurity policy, practices and activities at the TSO level. It is worth to mention that due to the specific functions of the TSOs and their participation in provision of essential services, both electricity and cybersecurity legislation were analyzed. The investigation considered eight countries from the SEE region [40], i.e., the Western Balkan countries, that are also Contracting Parties of the Energy Community Treaty (EnC CPs)—Bosnia and Herzegovina (BiH), North Macedonia, Montenegro and Serbia, and EU Member States (EU MSs)—Bulgaria, Croatia, Greece and Romania. The observed region is rather complex in terms of the level of implementation of the EU energy and cybersecurity legislation. The EnC CPs are not obligated to implement the EU legislation as they are not members of the Union. However, by signing the Energy Community Treaty, these countries have agreed on early adoption of parts of the EU energy acquis, thus aiming to bridge the gaps between the EU targets and current national legislation.

2.2. Cybersecurity Practices

The legislation analyses are combined with information collected from a survey that was designed to capture the implementation of legislative obligations as well as to provide insight into the technical solutions used by TSOs in terms of cybersecurity risk assessment, information security policies in place, practices to limit external access to CIs, assets protection and defense, and cooperation with national entities responsible for prevention and coordination of cybersecurity as Computer Incident Response Teams (CSIRTs). The survey also provided useful information on the implementation of the Network and Information systems (NIS) Directive [29]. An overview of the topics of the survey is presented in Table 1 below and further details on the survey data is available in [1,40].

Systems **2021**, *9*, 39 5 of 21

Table 1. Survey topics related to CI and assets.

Risk Management, Cyber Protection and Defense

Risk-assessment procedures and recommendations from the assessment
Existence of company information security policy
Development and maintenance of inventory of assets considering critical systems as well,
Maintenance of a list of companies with access to critical infrastructure systems (CIS) and
existence of special procedures for these companies when accessing CIS,
Implementation of measures to mitigate threats and external access on CIS, limitation of access
rights to users and automatic processes to CIS,

Implementation of measures to secure ICS and approaches in detection of threats to CIS, Existence of reporting procedures to Computer Security Incident Response Teams (CSIRTs), procedures for notification neighboring TSOs about cyber incidents, Existence of Security plan for protection of CIS.

3. Results

3.1. Analyses of the EU Legislative Framework

The EU legislation on cybersecurity encompasses several regulations, directives and other acts developed to increase cybersecurity at the national and EU level and increase EU cooperation on cybersecurity issues. The general character of the cybersecurity regulatory framework is horizontal and intersectoral. However, due to the specifics of transmission systems, it is also necessary to create links to electricity legislation. This section provides a comprehensive overview of all the acts that regulate the obligations of TSOs in cybersecurity.

3.1.1. NIS Directive

The central act in cybersecurity legislation is the NIS Directive [29], which has the objective to increase the capability of EU MSs and EU to build a systematic approach in counteracting possible threats to networks and information systems. An essential aspect of the NIS Directive is designation of Operators of Essential Services (OESs) and Digital Service Providers across the EU in a coherent manner. The objective of their identification and designation is to ensure that they implement the required technical and organizational measures to manage the risks of the networks and information systems they use and operate. According to the NIS Directive, TSOs are OESs and they are obligated to introduce these measures in their operation. The NIS Directive also stipulates designation of one or more national CSIRTs, National Competent Authorities (NCAs) and Single Points of Contact (SPOCs).

The EU MSs may designate one or more NCAs and their responsibility is to monitor the implementation of the NIS Directive at the national level, with tasks ranging from incident reporting, setting security measures, receiving and handling incident notifications, supervision in implementation of the Directive and identification of OESs. The SPOCs are responsible for maintaining cross-border cooperation between EU MSs with regards to incidents notifications. The NCA and the SPOC are the same entity if only one NCA is designated on national level. The designated national CSIRTs are responsible for monitoring and responding to incidents, providing early warnings, performing risk and incident analysis and participating in the CSIRTs Network. This network is established to facilitate cooperation on incident reporting between the EU countries. The cooperation at the EU level is ensured by establishment of the NIS Cooperation Group [29] consisting of representatives of EU MSs, the EC and the ENISA.

The major implementational barrier of the NIS Directive is related to fragmented approaches in designation of national OESs [41] and Digital Service Providers. Consequently, there is an absence of clear specification of security measures to be implemented by these entities. This impedes the expected effects of the directive. The incidents notification process requires improvements to facilitate sharing of information on cross-border incidents and increase the level of trust among the involved entities. In fact, there is still a lack of

Systems **2021**, *9*, 39 6 of 21

situational awareness and joint response at the EU level. This is of utmost importance for TSOs, as the implications of cross-border effects of cyber incidents may be significant, which is already discussed in the introductory section of the paper.

3.1.2. Cybersecurity Act

The Cybersecurity Act [30] is the EU Regulation that is designed to complement the NIS Directive, introducing two new key aspects: a permanent mandate for ENISA and EU rules for certification of products, processes and services. Regarding cybersecurity issues, ENISA should contribute to the development of a cooperative response to large-scale cross-border incidents and crises related to cybersecurity at the national and EU levels. With regards to TSOs as designated OESs, ENISA should cooperate with EU MSs and industry in the development of the technical aspects of the security requirements for OESs in accordance with existing standards and the NIS Directive provisions. The second aspect of the Cybersecurity Act is related to certification of products, services and processes under common certification procedures. This is especially important for the industry, as it will introduce certification procedures across the EU, which should also contribute to introducing accountability for cyber incidents among vendors and technology providers.

In fact, the certification under common procedures is also the major implementational challenge of the Cybersecurity Act. The process is envisaged as formal evaluation of ICT products, services and processes performed by a certification entity. The aim of the process is to confirm the level of compliance of products, services and processes with predefined criteria. The candidate certification schemes are prepared by ENISA upon request of the European Commission. Their development also includes relevant stakeholders as the European Union Cybersecurity Certification Group and Stakeholder Cybersecurity Certification Group. Given the process of digitalization and increased use of ICT products, services and processes in various sectors, it is challenging and complex to encompass the various cybersecurity vectors involved; to clearly define the scope; and to avoid unnecessary burdens in the tangled supply chains (for example various components are used to build ICS and other devices used in transmission systems).

3.1.3. Blueprint for Rapid Emergency Response

The Blueprint for rapid emergency response [31] has been adopted in 2017 to facilitate fast and effective response to large-scale cybersecurity attacks. The core objectives of the Blueprint are to enable effective response using all available national mechanisms, to share understanding of events by relevant stakeholders on the technical, operational and political levels and to agree on key public communication messages. These objectives should be achieved based on the principles of proportionality, subsidiarity, complementarity and confidentiality of information. The Blueprint also introduces obligations for technical cooperation on ENISA, CSIRTs Network and the Computer Emergency Response Team for the EU institutions (CERT-EU). This is a very important aspect of the act, as it engages the major actors in cybersecurity at the EU level.

3.1.4. Critical Infrastructure Directive

While not directly dealing with the issue of cybersecurity, the Critical Infrastructure Directive [32] lays down the concept of CIs and their physical protection. The objective of the Directive is to establish a common framework for identification and designation of European Critical Infrastructures (ECIs) as well as to establish the basis for their protection. The Directive addresses two essential sectors—energy and transport. However, since its adoption in 2008, according to its review [42], the objective is not entirely fulfilled. In addition, the circumstances and threats have changed significantly in the past decade. However, it is essential to note that the Directive has provided the environment for improvement of national legislation as well as increasing the awareness of all stakeholders in EU MSs that had no obligations for protection of CIs prior the transposition of this Directive. Significant

Systems **2021**, *9*, 39 7 of 21

activities have been performed to initialize and achieve protection of ECIs, which in some EU MSs expanded to building resilience as well. Section 3.1.5. Clean Energy Package.

3.1.5. Clean Energy Package

The recently adopted Clean Energy Package introduces specific provisions on cyber-security for the actors in the electricity sector through the Regulation (EU) 2019/941 on risk-preparedness in the electricity sector [33] and the Regulation (EU) 2019/943 on the internal market for electricity [34]. The Regulation on risk-preparedness recognizes cyber-attacks as risks and ensures that they are properly accounted for in the risk-preparedness plans. It stipulates the development of national and regional crisis scenarios, taking cyber-threats into consideration. TSOs, as major stakeholders, have an important role in the development of these scenarios. The Regulation on internal market of electricity [34] introduces cybersecurity within the tasks of the European Network of Transmission System Operators for Electricity (ENTSO-E) and of the EU distribution system operators' (EU DSO) entity. Namely, ENTSO-E has the task to promote cybersecurity and the tasks of EU DSO entity include data management, data protection and cybersecurity in cooperation with relevant authorities and regulated entities. The Regulation on the internal market for electricity also sets a requirement for development of a Network Code on Cybersecurity.

As these acts were adopted recently, it is quite early to analyze the effects of their implementation. For example, the methodology for identifying regional electricity crisis scenarios in accordance with Article 5 of Regulation (EU) 2019/941 was adopted in March 2020, so its application for crisis scenario identification has just begun.

3.1.6. Recommendation on Cybersecurity in the Energy Sector

The European Commission Recommendation on cybersecurity in the energy sector [35] considers the real-time requirements of the energy systems, the possibility of cascading effects and the existence of legacy and state-of-the-art technology. The Recommendation also identifies the main actions that should increase cybersecurity preparedness in the energy sector. With regard to real time operation, this Recommendation proposes that OESs implement the most recent international standards for real-time communication, cybersecurity and installations. They need to provide additional physical protection on legacy installations so that overall high level of cybersecurity is reached. The system operators are obligated to carefully consider the possible vulnerabilities when connecting legacy and new equipment; conduct risk analyses on legacy equipment; update software and hardware whenever possible; enable automated monitoring and analysis capability for legacy and Internet of Things devices and take measures against attacks coming from maliciously controlled consumer devices and applications [35]. The Recommendation on cybersecurity in the energy sector [35] proposes that network operators, especially designated OESs along with other relevant stakeholders, should assess their interdependencies and criticality in case of a successful cyberattack. They should set structured communication procedures, including communication with CSIRTs, which is in line with the NIS Directive.

3.2. Further Developments of the Legislation in the EU

Aside from the positive effects that the NIS Directive has on the increase of the level of cybersecurity across the EU, it showed certain weaknesses in implementation as already discussed in the previous sections. The NIS Directive does not set specific enough criteria for cybersecurity measures and identification of OESs and Digital Service Providers, which ultimately led to insufficient harmonization of the cybersecurity frameworks adopted at the national level. Although it addresses several sectors, the inter-sectoral dependencies are not entirely captured. Also, the top-to-bottom impacts (vertical links between various actors) within the considered sectors are not addressed adequately to ensure accountability in the multi-actor environment.

To account for these issues, the European Commission has already developed a proposal for a Directive on measures for a high common level of cybersecurity across the Systems **2021**, *9*, 39 8 of 21

Union, repealing the Directive (EU) 2016/1148 [43]. The proposal includes a number of requirements including setting national cybersecurity frameworks; introducing measures to facilitate strategic cooperation and exchange of information among EU MSs and among designated entities; information sharing arrangements; as well as introducing the obligation for performing risk management by all entities in the scope of the proposal.

To address the new challenges for the ECIs, the European Commission has developed a proposal for a Directive on the resilience of critical entities [44]. The proposal, which was prepared in 2020, introduces the requirements for national frameworks and strategies on the resilience of critical entities; addresses the identification of ECIs and the establishment and designation of competent authorities; introduces the obligations of critical entities in terms of risk assessment; defines disruptive events and incident information sharing requirements; and introduces measures to facilitate EU level cooperation.

As discussed above, the Regulation on internal market for electricity stipulates adoption of a Network Code on Cybersecurity with rules on minimum requirements, planning, monitoring, reporting and crisis management. The Network Code on Cybersecurity is under development. The Smart Grid Task Force Expert Group 2 [45] proposes that the Network Code should have the following structure: provision of a baseline protection for energy systems operators with minimum security requirements and setup of information security management systems in accordance with the ISO/IEC 27001:2013, the ISO/IEC 27002:2013 and the ISO/IEC 27019:2017 standards for risk management; advanced cybersecurity for energy OESs; and supportive elements and tools.

3.3. Analyses of the Legislative Frameworks in the Western Balkans

The Western Balkan countries lack a consistent approach in identification and designation of CIs, their protection, as well as providing adequate protection of networks and information systems. These countries are faced with the same potential risks as EU MSs; hence, they should develop legislation that will set the principles for achieving a high level of cybersecurity. The EnC Secretariat has started the activities to overcome regulatory gaps inside the EnC, as well as towards the EU. For this purpose, the Procedural Act 2018/2/MC-EnC [46] was adopted. It transfers some of the obligations from Critical Infrastructure Directive [32] and from the NIS Directive [29] to the EnC CPs. These obligations include establishment of a coordination group for cybersecurity and CI within the EnC with the aim to promote high level security of network and information systems and of CI. Furthermore, the Procedural Act 2018/2/MC-EnC [46] introduces the obligation for designation of one or more NCAs and SPOCs for the security of network and for CIs by EnC CPs and designation of one or more national CSIRTs. The Procedural Act 2018/2/MC-EnC [46] also introduces obligations on the EnC CPs to identify CIs in CPs and to report on the applied security measures and operator security plans.

3.4. Analyses of the Obligations of TSOs in SEE Emerging from the Current Legislative Frameworks

The cybersecurity regulatory framework sets the obligations of various actors and incorporates intersectoral dependencies that are typical for cybersecurity issues. Figure 1 presents both the complexity and complementarity of the cybersecurity regulative framework. The cybersecurity obligations for TSOs generally emerge from the obligations they have as OESs, designated CIs and the provisions of the electricity related legislation.

According to [41], all TSOs of the EU MSs in the observed region are identified as OESs. As for the EnC CPs, the process of identification of OESs is generally related to the process of identification of critical information infrastructures (CIIs) and is already an obligation from the Procedural Act 2018/2/MC-EnC [46]. From the observed region, Serbia is the most advanced, having laid down the criteria for identification of OESs in the electricity sector, although the process for designation is not completed yet [40,47]. BiH and North Macedonia have started the process for developing identification criteria, while Montenegro has not started this process at all [40,47]. The criteria for identification of CIs are already established in Serbia and the process has started in Montenegro [47].

Systems **2021**, *9*, 39 9 of 21

The process of designation is not completed in Serbia yet. BiH and North Macedonia have not started the process yet [40]. As identification and designation of OESs and CIs are necessary in order to apply the other provisions of the relevant legislation, it is essential that the EnC CPs complete these processes as soon as possible.

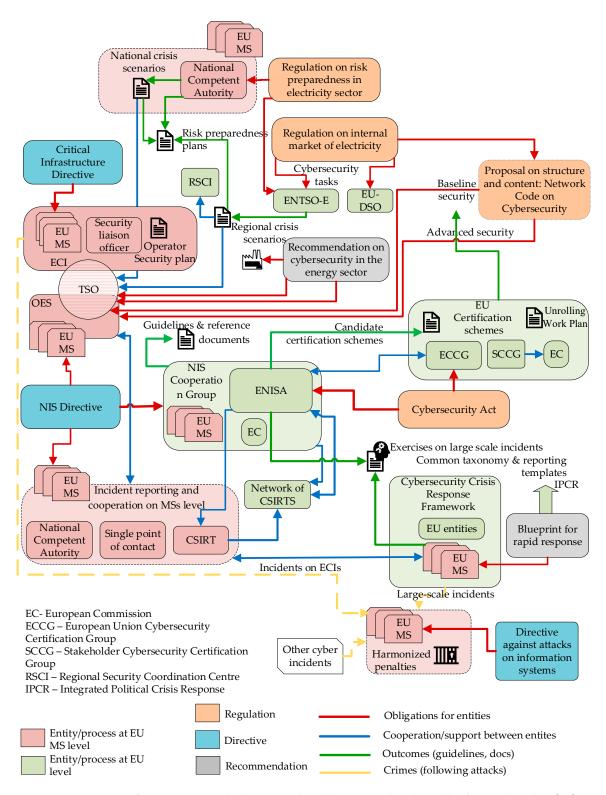


Figure 1. Overview of major actors and relations in the cybersecurity legislation landscape, based on [14].

Systems **2021**, *9*, 39 10 of 21

Related to the NIS Directive, the survey showed that all of the observed EU MSs have established NCAs, SPOCs and CSIRTs. However, the process of establishment of these entities is not completed in the EnC CPs. These countries usually have a national authority responsible for cybersecurity issues, but the obligations of these authorities emerge from various national legislative acts and are not necessarily consistent with the obligations of NCAs. Still, these authorities can streamline the activities of TSOs and national CSIRTs in the EnC CPs, in response to cyber incidents. The observed EnC CPs have established national CSIRTs [40], but these entities are not participating in the European Network of CSIRTs, which is the link between designated CSIRTs and ENISA.

Apart from the NIS Directive and the Critical Information Directive, most of the other direct cybersecurity obligations for TSOs emerge from the Recommendation on cybersecurity in the energy sector. This conclusion is easily derived by observing the scheme presented in Figure 1. The link between the Recommendation on cybersecurity in the energy sector and the NIS Directive is the obligation for TSOs to report the cyber incidents in case of cascading effects. Furthermore, the Recommendation on cybersecurity in the energy sector [35] stipulates development of risk preparedness plans based on crisis scenarios, which are established by cooperation among TSOs and other relevant stakeholders of the electricity sector. The preparedness plans include cyber-attacks among extreme circumstances for which the TSOs should be prepared. The Recommendation on cybersecurity in the energy sector is not obligatory for the EnC CPs.

Incident Notification and Reporting Process

As discussed above, the process of incident notification should be established at each TSO, by developing an internal procedure that will enable determining the significance of the incident and start the notification process. The recommendations for determining the significance should be based on reference documents from the NIS Cooperation Group [48]. The notification and reporting process also includes other entities, i.e., NCAs, SPOCs and CSIRTs, as shown in Figure 2. For simplification, they are shown in a common box, but the actual notification of the incident is sent to the NCA and/or the designated CSIRT, which is discussed in more detail further in the text. The SPOC is responsible for notifying the SPOC in the neighboring country.

The process depends strongly on the national setup and the designated responsibilities of all stakeholders. The TSO should apply a consistent risk-management procedure to tackle cyber threats and at the same time, it should develop procedures for determining the incident significance. These procedures should be simple enough to conduct, as they would be run at the same time when the incident occurs. The NCAs/CSIRT should develop templates for incident notification (check-box lists, fill-in templates) and ensure that there are at least two possible methods for notification. This is important because of the possibility of limited access of some of the ICT infrastructures by the TSO. Sending confirmation to the TSO upon receiving the notification would ensure the flow of information. On national level, it is essential that all stakeholders have clear roles and responsibilities in the process. As the implementation of the NIS Directive ensures the setup and distribution of roles, the EnC CPs should consider full transposition of the NIS Directive into their national legislation. Until this process is completed, the EnC CPs should distribute the roles and responsibilities among the existing stakeholders, preferably using national CSIRTs as entities that receive notifications on incidents. An example of good practice is the established cooperation of the Greek electricity utilities with their national CSIRT. The survey showed that they participate in frequent national cyber security exercises organized by the national CSIRT, which is considered an efficient tool for network security assessment at the organizational level [40].

Systems **2021**, 9, 39 11 of 21

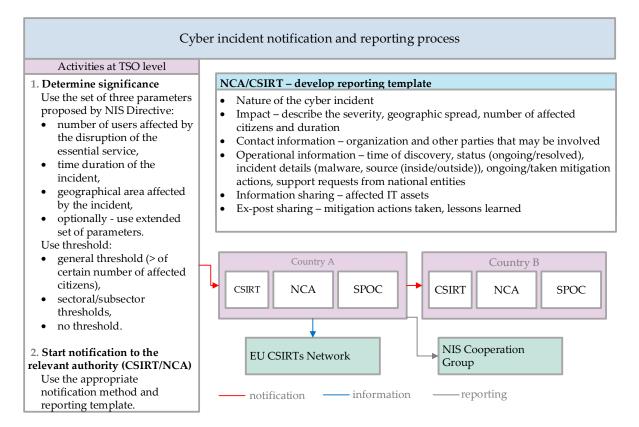


Figure 2. Cyber incident notification and reporting, based on [14,48,49].

3.5. Analyses of Practices for Security of Assets and CIIs

Maintaining security of CIIs and assets is only possible by implementation of adequate policies at the TSO level and implementation of information security management systems, i.e., the ISO/IEC 27,000 family of standards. In this subsection, the results of the investigations and the survey that included the TSOs of the observed SEE region are presented in a descriptive manner and anonymously, due to confidentiality of some of the data.

3.5.1. Risk Management of Threats

Risk assessment is essential in the risk-management process and should be performed regularly, throughout the whole life cycle of the CIIs. However, the analyses of the survey data [40] show that regular risk assessment is not a common practice for the TSOs in the observed region since only two of them apply it on regular basis. Consequently, only two TSOs are implementing the measures derived from the risk assessment process. Nevertheless, the results from the performed survey show that the TSOs plan to perform risk-assessment regularly in the future. In fact, performing risk assessment is recommended for developing tailor-made measures for risk mitigation for each TSO. The survey also showed that the majority of the TSOs create and maintain lists of CIIs and assets.

3.5.2. Mapping of Assets and Threats

The lists of TSO assets that relate to information systems include: physical components of the transmission system (cables, relays, transformers, switches, automation, sensors, FACTS devices, etc.); operational information about electrical assets (status indicators, alerts, events, disturbance information); historical information (data that is stored for further use/or as legislation requirement); trending information (all information related to commercial issues); and information system configuration (communication network topology, Internet Protocol addresses, Media Access Control addresses, user credentials & permissions, configuration files, location data). Apart from these assets, the information

Systems **2021**, *9*, 39

and control systems implemented by the TSOs use software, services, SCADA components and other hardware components.

Among the major recommendations for the TSOs related to the security of their assets is to maintain and regularly update their lists of assets and map these assets to possible threats. The threats may be related to intrusions during data transfer among assets, software malfunctions and bugs, user errors, field assets malfunctions, communication equipment malfunctioning/failures, physical attacks (physical destruction of equipment), system intrusion and abuse of data [50]. ENISA has introduced the main categories of threats for 2020 [51] as follows: malware, web based/web application attacks, social engineering (phishing, spam), distributed denial of service, identity theft, data breach, insider threat, botnet, physical manipulation and damage, information leakage, ransomware, cyberwarfare/espionage and cryptojacking.

Mapping the assets to possible threats will create a useful tool that provides inputs for determining the significance of an incident as well as for the risk-assessment process. The mapping should consider the assets in operation, past experiences, threat analyses and expected impacts on the system. A general depiction of such an exercise is presented in Figure 3 which shows how specific threats can be matched with different categories of assets, differentiating among threat risk levels in the process. According to [47], the highest risks for the TSOs emerge from malware, social engineering, including phishing and spam, insider threats, espionage, ransomware and botnet. The web-based attack risks are considered as medium, while the denial-of-service threat risks are considered as low. Except web-based and denial of service threats, all other threats pose high risks for cascading. Therefore, using the proposed mapping system presented on Figure 3, the threats for level 1 equipment may include insider threat (Threat 1) and cyberespionage (Threat 2). The number and level of risks of threats could change based on the assessments of the TSOs.

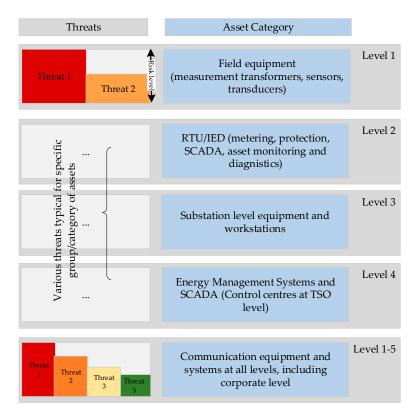


Figure 3. Mapping of assets and threats.

The main difficulty in this process is uncovering potential threats in a realistic manner. According to [52], the process of threat intelligence management requires several steps that

Systems **2021**, *9*, 39

start with adequate planning, which sets the general requirements and security goals. Then, data on possible threats is identified, collected and processed, considering the requirements and goals set in the previous step. The collected data is analyzed and shared among the utilities (in this case TSOs). Sharing of information on threats is the key step in the whole process but is often avoided due to the sensitivity of data. In fact, a similar observation is made in [53], noting that the current approach for sharing information within interest communities is not efficient enough. Sharing information within networks of trust, such as the European Energy—Information Sharing and Analysis Centre (EE-ISAC) is proposed as an adequate approach in [52], which is also envisaged within the jurisdiction of the EnC. The initiative for EnC-ISAC is presented in [54] and envisions that the ISAC would be established by both public (state owned) and private operators of energy utilities and infrastructures with the aim to help them protect their assets from cyber and physical threats by analyses and dissemination of threat information among the members and partners of the ISAC. In addition, novel approaches for threat analytics that use data mining, correlation of shared data and automated threat discovery should complement the existing solutions for uncovering threats, their modeling, analysis, remediation and mitigation [52].

The threat landscape is becoming even more complex if the supply-chains and logistic-chains are considered. TSOs usually procure equipment from various vendors based on the requirements they set on quality and depending on the offered price of the equipment. In this way TSOs benefit from the competition between vendors and avoid being dependent on a single equipment supplier. Under these circumstances, it is difficult to ensure the integrity of the supply-chain and uncover threats related to vulnerabilities of specific equipment components. Therefore, it is necessary to implement existing good practices consistently, especially in the procedures for equipment purchase. The certification of products, services and processes should increase the trust in supply and logistic-chains.

3.5.3. Protection of CIIs and SCADA

Figure 4 provides an overview of the cybersecurity protection measures of critical systems applied by the TSOs in the observed region. The data presented in Figure 4 was collected through the survey and depicts the implemented measures for minimization of external access to CIIs, on architectural and system administration level. The measures at the top of the lists presented in Figure 4 are the most used among the TSOs and the bottom ones are the least used.

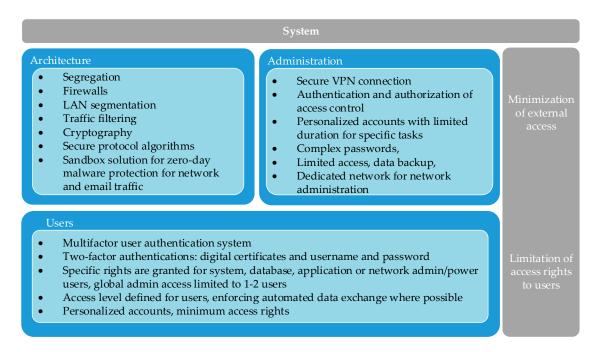


Figure 4. Overview of system architecture and system administration for protection of CIIs used by the TSOs in SEE.

Systems **2021**, *9*, 39 14 of 21

Generally, implementation of segregation and firewalls are among the most common measures along with traffic filtering and anti-malware. The administration work on CIIs is performed using accounts that impose certain restrictions (time duration limit, password protection, access restrictions). Although the unauthorized external access is critical for protection of CIIs, the internal access of users with certain administrative and operational privileges is also controlled. As depicted in Figure 4, the common approach is to implement multifactor user authentication, but also specific access rights for users undertaking tasks in the CIIs environment are used (definition of various access levels for various types of users, personalized accounts, minimum rights for access). A common approach for the TSOs in the region is implementation of segregation of the SCADA systems from other CIIs, but also implementation of firewalls and restriction to the internet access. From the analyses of the collected data, it can be concluded that the TSOs in the region use standard technical solutions to protect their assets, CIIs and SCADA systems.

Based on the analysis of the collected data, the major recommendation is to ensure consistency of these measures across critical assets. The users (employees) should be motivated and trained in maintaining the required level of vigilance. Furthermore, strict rules should apply to external parties with access to the CIIs, and at the same time, the TSOs should maintain lists of all active external parties. The survey showed that the general trend among the TSOs is to maintain these lists and apply measures against unauthorized access and use of CIIs. Similar to the other measures, these are considered standard measures for limitation of external access and for limitation of access for users. The most important recommendations for efficient protection of SCADA systems are to align protection measures among SCADA/ICS and CIIs, to build cybersecurity awareness and to foster expertise among users.

4. Discussion

The analyses of the current TSO practices are based on an extensive survey undertaken by the TSOs in SEE, which helped uncover the gaps in their corporate cybersecurity policies. From the analyses it is obvious that the TSOs in the SEE region apply standard technical measures to protect and defend their information infrastructures. However, most of them lack an organized approach in developing a consistent and sustainable cybersecurity company policy. The establishment of such a policy ensures incorporation of the obligations and recommendations from both cybersecurity and electricity legislation. Furthermore, implementation of advanced cybersecurity measures for contemporary and future CPPSs can only start when basic cybersecurity measures and policies are in place. This section provides a proposal for improvements of TSOs cybersecurity practices and bridging any inconsistencies in their cybersecurity approach.

Proposal for Improvements of TSO Cybersecurity Practices

Figure 5 presents a proposal for a TSO cybersecurity framework, based on the investigations of the observed SEE region [14]. The establishment of a cybersecurity framework on a company level should improve the company's resilience to threats and attacks. The framework envisages that TSOs establish TSO cybersecurity team(s) and, if possible, a TSO cybersecurity center. The objective of the teams/center would be to coordinate the tasks and processes at company level.

According to the proposed framework, the TSO management would be responsible for the establishment of the cybersecurity team and the adoption of the cybersecurity policy based on recommendations from the TSO cybersecurity team. In this context, the TSO management should ensure the availability of resources for implementation of the TSO cybersecurity policy and should stimulate continuous education and specialization of the TSO cybersecurity team. The TSO cybersecurity team should be responsible for coordination of cybersecurity tasks and conduct the processes related to operational security. Among its major tasks would be the performance of a regular risk assessment, as a basis for developing an effective cybersecurity policy. The TSO cybersecurity team should be

Systems **2021**, *9*, 39 15 of 21

responsible for raising cybersecurity awareness at the company level and cooperating with national authorities and the designated CSIRT. To ensure adequate protection of critical infrastructure, the TSO cybersecurity team should have responsibilities for maintaining lists of assets, mapping the assets against possible threats, cooperating with the security liaison officer and ensuring the cybersecurity protection of these assets. This can be achieved by applying the cybersecurity measures for all products and systems, as shown in Figure 5.

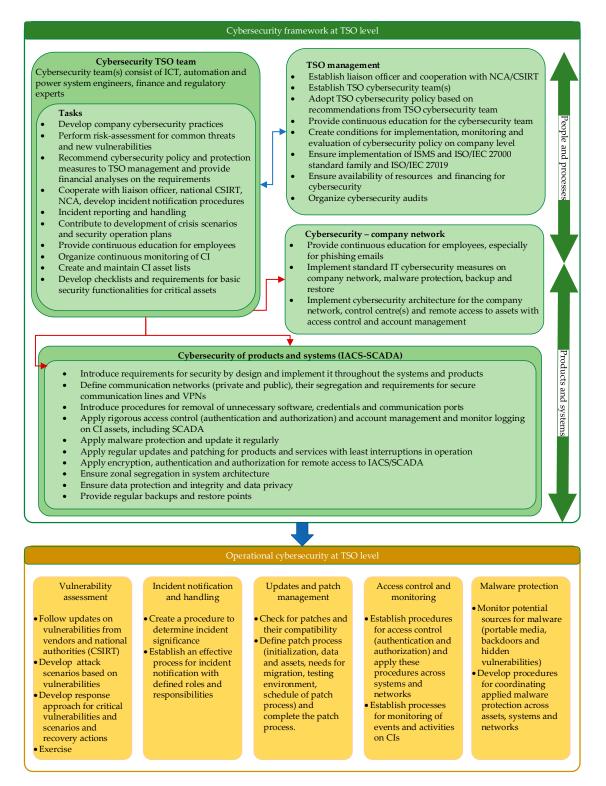


Figure 5. A proposal for TSO cybersecurity framework based on the investigations in [14].

Systems **2021**, *9*, 39 16 of 21

The proposed framework integrates risk-assessment, cybersecurity policy development and implementation, education of employees and auditing as well as revision of the established policy. Specific risk attack scenarios should be developed to capture the vulnerabilities, threats and possible actors capable of performing the attacks. Based on these analyses the likelihood of an attack can be assessed. The steps that should be taken in the risk-assessment process leading to design of TSO company specific policies are presented in Figure 6. The capability to assess the possible impacts should be used to prepare efficient procedures to determine incident significance, which is one of the steps in the notification procedure described in Figure 2.

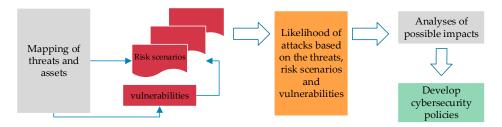


Figure 6. Risk-assessment process at TSO level, based on mapping of threats and assets.

The internal TSO governance model for implementation of the framework depends on the company organizational setup. A major recommendation in setting up the model is to consider the interdisciplinarity of the problem and to design the governance to make use of the high-level skills of employees from different sectors. A simplified model is presented in Figure 7, showing that the TSO cybersecurity center should cooperate with the ICT, operation and control, and planning sectors, as well as with the security liaison officer.

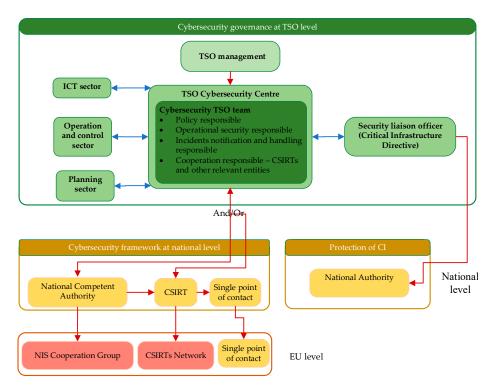


Figure 7. Proposal for cybersecurity governance model, based on the investigations in [14].

As depicted in Figure 5, the TSO cybersecurity team has numerous responsibilities aimed to improve the overall cybersecurity practices. From a governance aspect, the TSO cybersecurity team should be comprised of highly skilled personnel capable of completing the tasks of cybersecurity policy development, operational security implementation,

Systems **2021**, *9*, 39 17 of 21

incident reporting, cooperation with designated entities and other tasks. Therefore, the essential challenge for the TSO management is to establish a team and invest in its continuous training and education.

The governance model presented in Figure 7 is proposed under the assumption that the TSOs have sectors/departments responsible for planning, operation and control and ICT. The cooperation of the TSO cybersecurity center with the ICT sector ensures exchange of knowledge between the IT and operational technology security experts, considering the possible differences in applied cybersecurity measures in ICT and SCADA systems. In fact, the cooperation between IT and operational technology experts becomes a requirement as operational safety and cybersecurity requirements converge. The monitoring and control functions are essential for the TSO operation and control sector, but also, these functions may be used to uncover suspicious behavior and intrusions. The expertise of employees in the TSO operation and control sector should be used in the design of the cybersecurity protection measures as well as in development of risk scenarios. The cooperation between the TSO cybersecurity center and the planning sector is also important for the development of risk scenarios and for taking into account future developments of the transmission system. A coherent cybersecurity policy at the organizational level can be accomplished only by strong cooperation between sectors and considerable investment in people and their skills

The proposed governance model is in line with the requirements for OESs set by the NIS Directive. The TSO cybersecurity team is also responsible for establishing cooperation with the national authorities and sharing information on cyber incidents. Through the cooperation with the NCA and CSIRT, the EU level relations are established. The proposed governance model does not set limits for sharing information within networks of trust, such as the ISAC. As discussed in the previous section, sector based ISACs provide significant support to system operators in dealing with imminent threats. TSO Security liaison officer cooperates with the designated national authority on the matters related to protection of CIs, as recommended in the Critical Infrastructure Directive.

The proposed TSO cybersecurity framework and governance model are developed based on the collected data and existing practices of TSOs. The expected implementation challenges may emerge from limited capacity of resources and people, i.e., financial requirements to provide the necessary analytical tools for the TSO cybersecurity team and to provide adequate training for both IT and operational technology specialists. The organizational set-up is not complex, so the simplest approach is to combine the skills of experts from ICT and operational technology when establishing the TSO cybersecurity center. The increase of the TSO cybersecurity center operational capacity would be a continuous process that depends on the current TSO capacities as well as on the commitment of the management of the company to provide resources and support for the implementation of the proposed framework. The cooperation between the various sectors/departments is also an organizational issue which would not increase the complexity of the proposed framework. With regards to the EnC CPs, the challenges are also related to implementation of the required legislation as stipulated in the Procedural Act [46]. However, the proposed framework would only help the TSOs from EnC CPs to adjust and improve their practices. The proposed cybersecurity framework and governance model are envisaged as a solution that would bridge the existing cybersecurity gaps as well as prepare the TSOs for future innovative solutions and new requirements emerging from upcoming legislative developments.

5. Conclusions

The paper presents results from the analyses of the implementation of cybersecurity policies and protection measures by TSOs in the SEE region and clearly demonstrates the necessity to increase the cybersecurity capabilities of TSOs. It includes a comprehensive analysis of the EU cybersecurity legislation as well as analysis of the cybersecurity requirements emerging from the electricity legislation, focusing on the obligations for

Systems **2021**, *9*, 39 18 of 21

TSOs. The analyses imply that the implementation of the regulatory framework varies in maturity across the region. The EnC CPs should accelerate the process of transposition of the necessary legislation, designate the TSOs as OESs and designate the other entities, including NCAs and SPOCs. The analyses show that the differences between TSOs from the EU MSs and the EnC CPs are not very significant with regards to the applied technical solutions for defense and protection of CIIs and assets. The main differences are related to the implementation of cybersecurity risk-assessment, which is performed regularly only by two TSOs in the observed region.

It can be concluded that there is a necessity to create an adequate environment at the company level to develop and maintain sustainable policies that will address current and emerging threats. Therefore, the paper proposes a cybersecurity framework and governance model that should improve the overall TSO response to threats and attacks. The proposed framework is developed considering the inputs from TSOs and aims to improve their existing cybersecurity practices. The proposed cybersecurity framework for TSOs is based on a holistic approach that integrates people and their skills, processes and products. It introduces the necessary requirements for ensuring security of products and assets at the process level. The proposed framework also outlines the tasks and activities that need to be carried out at corporate level. Furthermore, to ensure a harmonized approach, the framework is linked to a proposed TSO governance model, which is compliant with the requirements from the EU cybersecurity legislation.

Author Contributions: Conceptualization, A.K.M., P.K. and S.B.; methodology, P.K. and S.B.; software, P.K.; validation, A.K.M., P.K. and S.B.; formal analysis, A.K.M.; investigation, A.K.M., P.K. and S.B.; resources, A.K.M., P.K. and S.B.; data curation, P.K. and S.B.; writing—original draft preparation, A.K.M.; writing—review and editing, P.K. and S.B.; visualization, A.K.M.; supervision, A.K.M.; project administration, P.K.; funding acquisition, A.K.M. and P.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by EU H2020 project CROSSBOW, grant number 773430.

Acknowledgments: The authors would like to acknowledge the support of colleagues from system operators, who took part in the survey and kindly shared their knowledge and experience.

Conflicts of Interest: The authors declare no conflict of interest. This paper reflects only the authors' views and neither the Agency nor the Commission are responsible for any use that may be made of the information contained therein.

Abbreviations

BiH Bosnia and Herzegovina

CERT-EU Computer Emergency Response Team for the EU institutions

CI Critical Infrastructure

CII Critical Information Infrastructure

CP Contracting Party

CPPS Cyber-Physical Power Systems
CSIRT Computer Incident Response Teams
ECI European Critical Infrastructure

EE-ISAC European Energy – Information Sharing and Analysis Centre

EMS Energy Management Systems

EnC Energy Community

ENISA European Union Agency for Cybersecurity

EU European Union

EU-DSO EU distribution system operators' entity

ENTSO-E European Network of Transmission System Operators for Electricity

ICS Industry Control Systems

ICT Information and communication technologies

Systems **2021**, 9, 39 19 of 21

OES Operator of Essential Services

MS Member State

NCA National Competent AuthorityNIS Network and Information SystemsSADA Supervisory Control and Data Acquisition

SEE South East Europe
SPOC Single Point of Contact

TSO Transmission System Operator

References

 Krkoleva Mateska, A.; Krstevski, P.; Borozan, S. Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats. In Proceedings of the 15th Conference on Sustainable Development of Energy, Water and Environment Systems (SDEWES), Cologne, Germany, 1–5 September 2020. paper ID 0620.

- 2. Yohanandhan, R.V.; Elvarasan, R.M.; Manoharan, P.; Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis with Cyber Security Applications. *IEEE Access* **2020**, *8*, 151019–151064. [CrossRef]
- 3. Krkoleva Mateska, A.; Krstevski, P.; Borozan, S. Cybersecurity Protection and Defence Measures in the Electricity Transmission Networks in South East Europe. In Proceedings of the ICEST 2019, Ohrid, North Macedonia, 27–29 June 2019. Available online: https://icestconf.org/wp-content/uploads/2019/09/Proceeding_ICEST_2019.pdf (accessed on 16 May 2021).
- 4. CROSSBOW Project. Available online: http://crossbowproject.eu/ (accessed on 10 April 2020).
- 5. Desarnaud, G. Cyber Attacks and Energy Infrastructures: Anticipating Risks, Études de l'Ifri, January 2017. Available online: https://www.ifri.org/en/publications/etudes-de-lifri/cyber-attacks-and-energy-infrastructures-anticipating-risks (accessed on 20 March 2020).
- 6. Hossain, M.M.; Peng, C. Cyber–physical security for on-going smart grid initiatives: A survey. *IET Cyber-Phys. Syst. Theory Appl.* **2020**, *5*, 233–244. [CrossRef]
- 7. Livingston, S.; Sanborn, S.; Slaughter, A.; Zonnenveld, P. Managing Cyber Risk in the Electric Power Sector: Emerging Threats to Supply Chain and Industrial Control Systems, Delloite. Insight. 2018. Available online: https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf (accessed on 10 April 2020).
- 8. ENISA. The Cost of Incidents Affecting CIIs, Systematic Review of Studies Concerning the Economic Impact of Cyber-Security Incidents on Critical Information Infrastructures (CII), August 2016. Available online: https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis (accessed on 20 April 2020).
- 9. Borges Hink, R.C.; Beaver, J.M.; Buckner, M.A.; Morris, T.; Adhikari, U.; Pan, S. Machine learning for power system disturbance and cyberattack discrimination. In Proceedings of the 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 19–21 August 2014; pp. 1–8.
- 10. ENISA. Communication Network Dependencies for ICS/SCADA Systems, February 2017. Available online: https://www.enisa.europa.eu/publications/ics-scada-dependencies (accessed on 10 April 2020).
- 11. Daugulis, A. Cyber Security from TSO Perspective; Riga Workshop; USAID, NARUC: Washington, DC, USA, 2018.
- 12. Jimada-Ojuolape, B.; Teh, J. Impact of the Integration of Information and Communication Technology on Power System Reliability: A Review. *IEEE Access* **2020**, *8*, 24600–24615. [CrossRef]
- 13. ENSA. Main Incidents in the EU and Worldwide (January 2019–April 2020), October 2020. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents (accessed on 10 December 2020).
- 14. Krkoleva, A.; Borozan, V.; Krstevski, P.; Borozan, S. D8.4 Cyber Security Communication Procedures and Impact of Disruption Events. V1.0. May 2020. CROSSBOW Project, H2020-773430. Available online: http://crossbowproject.eu/deliverable-8-4/(accessed on 6 March 2020).
- 15. Soltan, S.; Yannakakis, M.; Zussman, G. Power grid state estimation following a joint cyber and physical attack. *IEEE Control. Netw. Syst.* **2018**, *5*, 499–512. [CrossRef]
- Lee, R.M.; Assante, M.J.; Conway, T. Analysis of the Cyber Attack on the Ukrainian Power Grid; SANS Industrial Control Systems & E-ISAC: Washington, DC, USA, 2016; Available online: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (accessed on 6 March 2020).
- 17. Teixeira, A.; Amin, S.; Sandberg, H.; Johansson, K.H.; Sastry, S.S. Cyber security analysis of state estimators in electric power systems. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5991–5998.
- 18. Ashok, A.; Wang, P.; Brown, M.; Govindarasu, M. Experimental evaluation of cyber-attacks on automatic generation control using a CPS security testbed. In Proceedings of the IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5.
- Mohan, A.M.; Meskin, N.; Mehrjerdi, H. A Comprehensive Review of the Cyber-Attacks and Cyber-Security on Load Frequency Control of Power Systems. *Energies* 2020, 13, 3860. [CrossRef]
- 20. Xie, L.; Mo, Y.; Sinopoli, B. Integrity data attacks in power market operations. IEEE Trans. Smart Grid 2011, 2, 659–666. [CrossRef]
- 21. Ayad, A.; Farag, H.; Youssef, A.; El-Saadany, E. Cyber–physical attacks on power distribution systems. *IET Cyber-Phys. Syst. Theory Appl.* **2020**. [CrossRef]

Systems **2021**, *9*, 39 20 of 21

22. Sukumara, T.; Sudarsan, S.D.; Starck, J.; Vittor, T.R. Cyber security—Security strategy for distribution management system and security architecture considerations. *CIRED Open Access Proc. J.* **2017**, 2017, 2653–2656. [CrossRef]

- 23. Li, L.; Wang, W.; Ma, Q.; Pan, K.; Liu, X.; Lin, L.; Li, J. Cyber attack estimation and detection for cyber-physical power systems. *Appl. Math. Comp.* **2021**, *400*, 126056. [CrossRef]
- 24. Carter, B.; Adams, S.; Bakirtzis, G.; Sherburne, T.; Beling, P.; Horowitz, B.; Fleming, C. A Preliminary Design-Phase Security Methodology for Cyber–Physical Systems. *Systems* **2019**, *7*, 21. [CrossRef]
- 25. Ngyen, T.; Wang, S.; Alhazmi, M.; Nazemi, M.; Estebsari, A.; Dehghanian, P. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. *IEEE Access* **2020**, *8*, 87592–87608. [CrossRef]
- 26. Sun, C.-C.; Liu, C.-C.; Xie, J. Cyber-Physical System Security of a Power Grid: State-of-the-Art. Electronics 2016, 5, 40. [CrossRef]
- 27. Kong, P.Y. Cost efficient data aggregation point placement with interdependent communication and power networks in smart grid. *IEEE Trans. Smart Grid* **2019**, *10*, 74–83. [CrossRef]
- 28. Yaacoub, J.-P.A.; Salman, O.; Noura, H.N.; Kaaniche, N.; Chehab, A.; Malli, M. Cyber-physical systems security: Limitations, issues and future trends. *Micropro. Microsyst.* **2020**, *77*, 103201. [CrossRef] [PubMed]
- 29. 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. Available online: http://data.europa.eu/eli/dir/2016/1148/oj (accessed on 12 December 2019).
- 30. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 523/2013, Official Journal of the European Union. 2019. Available online: http://data.europa.eu/eli/reg/2019/881/oj (accessed on 14 March 2020).
- Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity
 Incidents and Crises, Brussles: OJ L 239. 2017. Available online: http://data.europa.eu/eli/reco/2017/1584/oj (accessed on 14
 March 2020).
- 32. Directive 2008/114/EC—Identification and Designation of European Critical Infrastructures and Assessment of the Need to Improve their Protection. Available online: http://data.europa.eu/eli/dir/2008/114/oj (accessed on 14 March 2020).
- 33. 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, Brussels: OJ L 158, 2019. Available online: http://data.europa.eu/eli/reg/2019/941/0j (accessed on 20 April 2020).
- 34. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the Internal Market for Electricity (recast), Brussels: OJ L 158. 2019. Available online: http://data.europa.eu/eli/reg/2019/943/oj (accessed on 20 April 2020).
- 35. European Commission. *Commission Recommendation of 3.4.2019 on Cybersecurity in the Energy Sector*; European Commission: Belgium, Brussels, 2019.
- 36. Cooperation Group. Reference Document on Security Measures for Operators of Essential Services, CG Publication 01/2018. Available online: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed on 16 March 2020).
- 37. Huang, X.; Qin, Z.; Liu, H. A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access* **2018**, *6*, 69023–69035. [CrossRef]
- 38. Da Silva, L.E.; Coury, D.V. A new methodology for real-time detection of attacks in IEC 61850-based systems. *EPSR* **2017**, *143*, 825–833. [CrossRef]
- 39. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power system in a cyber-physical environment. *EPSR* **2017**, *149*, 156–168. [CrossRef]
- 40. Borozan, V.; Krkoleva, A.; Krstevski, P.; Taleski, R.; Borozan, S. D3.2 Privacy and Data Protection in a Multi-Actor Environment, V1.0, February 2019. CROSSBOW Project, H2020-773430. Available online: http://crossbowproject.eu/deliverable-3-2/ (accessed on 11 March 2020).
- 41. European Commission. COM (2019) 546 final, Report from the Commission to the European Parliament and the Council Assessing the Consistency of the Approaches taken by Member States in the Identification of Operators of Essential Services in Accordance with Article 23(1) of Directive 2016/1148/EU on Security of Network and Information Systems. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN (accessed on 14 March 2021).
- 42. European Commission. Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. 2019. Available online: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723 _swd-2019-308-commission-staff-working-document_en.pdf (accessed on 16 March 2020).
- 43. European Commission. Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148, COM/2020/823 Final. 2020. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823 (accessed on 2 April 2021).
- 44. European Commission. Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities, COM/2020/829 Final. 2020. Available online: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020 _proposal_directive_resilience_critical_entities_com-2020-829_en.pdf (accessed on 2 April 2021).

Systems **2021**, *9*, 39 21 of 21

45. Smart Grid Task Force Expert Group 2. Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Final Report June 2019. Available online: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf (accessed on 5 April 2021).

- 46. Procedural Act of the Ministerial Council of the Energy Community 2018/2/MC-EnC: On the Establishment of an Energy Community Coordination Group for Cyber-Security and Critical Infrastructure, 2018. Available online: https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf. (accessed on 10 March 2020).
- 47. Blueprint Energy Solutions GmbH. Study on Cybersecurity in the Energy Sector of the Energy Community; Blueprint Energy Solutions GmbH: Vienna, Austria, 2019.
- 48. NIS Cooperation Group. Reference Document on Incident Notification for Operators of Essential Services—Circumstances of Notification, 2018. Available online: https://energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf (accessed on 11 March 2020).
- 49. NIS Cooperation Group. Guidelines on notification of Operators of Essential Services Incidents, Formats and Procedures, 2018. Available online: https://digital-strategy.ec.europa.eu/en/library/nis-cooperation-groups-guidelines-implementing-nis-directive-and-addressing-wider-cybersecurity (accessed on 12 March 2020).
- 50. ENISA. Smart Grids Task Force EG2 Deliverable—Proposal of a List of Security Measures for Smart Grids. 2013. Available online: https://resilience.enisa.europa.eu/security-and-resilience-of-communication-networks-and-information-systems-for-smart-grids/eg2-minimum-security-measures-for-smart-grids/conference-calls/3rd-conference-call/final-document/view (accessed on 2 April 2021).
- 51. ENISA, Threat Landscape Report. 2020. Available online: https://www.enisa.europa.eu/publications/year-in-review (accessed on 6 April 2021).
- 52. Harsch, A.; Moulinos, K.; Seiler, A.; Skouloudi, A. Threat Intelligence Management: An EE-ISAC White Paper. 2020. Available online: https://www.ee-isac.eu/threat-intelligence-management-white-paper/ (accessed on 21 May 2021).
- 53. Stamp, J.E.; Quiroz, J.E.; Ellis, A.; Bhagyavati, B.; Cooley, J.A.; Dahl, K.; Limpaecher, E.R. Cyber Security Gap Analysis for Critical Energy Systems. 2017; SAND2017-1785. Available online: https://www.osti.gov/servlets/purl/1494189/ (accessed on 21 May 2021).
- 54. Energy Community. Establishment of Energy Community Energy ISAC—White Paper. June 2020. Available online: https://www.energy-community.org/dam/jcr:4e4513fa-f1d0-4238-abe6-7e2277ef0c9a/EnC%20_ISAC_072020.pdf (accessed on 21 May 2021).