energies

MDPI

Article

EE-ISAC—Practical Cybersecurity Solution for the Energy Sector

Tania Wallis [1,*] and Rafał Leszczyna [2]

[1] School of Computing Science, University of Glasgow, Glasgow G12 8RZ, UK
[2] Faculty of Management and Economics, Gdańsk University of Technology, Narutowicza 11/12, 80-233 Gdańsk, Poland; rafal.leszczyna@pg.edu.pl
* Correspondence: tania.wallis@glasgow.ac.uk

Abstract: A recent survey of cybersecurity assessment methods proposed by the scientific community revealed that their practical adoption constitutes a great challenge. Further research that aimed at identifying the reasons for that situation demonstrated that several factors influence the applicability, including the documentation level of detail, the availability of supporting tools, and the continuity of support. This paper presents the European Energy Information Sharing and Analysis Centre (EE-ISAC)—a cybersecurity platform for the energy sector that has been adopted by multiple organisations. The platform facilitates sharing information about cybersecurity incidents, countermeasures, and assessment results. Prospectively, it is envisaged to be integrated with the threat intelligence platform that enables real-time situational awareness. By considering both fault and attack scenarios together, threat awareness can be mapped onto operational contexts to prioritise decisions and responses. This paper analyses EE-ISAC's approach based on the conceptual applicability framework developed during the research, to improve the applicability and usefulness of this platform for energy sector participants and to identify areas that require further development.

Keywords: cybersecurity; information sharing; threat intelligence; situational awareness; applicability; organisational management

Citation: Wallis, T.; Leszczyna, R. EE-ISAC—Practical Cybersecurity Solution for the Energy Sector. *Energies* **2022**, *15*, 2170. https://doi.org/10.3390/en15062170

Academic Editor: Valentina Colla

Received: 9 February 2022
Accepted: 11 March 2022
Published: 16 March 2022

1. Introduction

Recently, a survey of cybersecurity assessment methods proposed by the scientific community was conducted [1]. Based on a systematic research method, 32 cybersecurity assessment methods were identified and investigated. The analysis revealed that despite the large number of proposals, their practical use in operational contexts is incidental. At the same time, the developments are limited to pilot or demonstration sites, hypothetical scenarios, or some preliminary configurations. Still, new solutions are being introduced. These observations were connected to the methods' applicability properties. For instance, the methods' documentation was not sufficiently detailed to facilitate the method's deployment and practical use. Additionally, indications of the time and effort necessary to employ a method were missing. Frequently, no tools were delivered to support the use of a method. The study acknowledged the importance of analysing the applicability of a solution when aiming at its broad uptake and continuous use. At the same time, it became evident that the research on applicability is in its initial stage. Existing research focuses on particular application domains or solely mentions metrics or determinants in the context of applicability [2–4].

The European Energy Information Sharing and Analysis Centre (EE-ISAC) is a cybersecurity platform that integrates energy sector stakeholders to exchange knowledge on threats, vulnerabilities, incidents, solutions, and opportunities. It was established in 2015, and from that time has attracted multiple organisations that joined its network of trust. The organisations include utilities (producers, transmission operators, and distributors); providers of security products and services; academia and research institutions; as well as governmental and non-governmental agencies. They share information during physical

meetings as well as using electronic means, including a dedicated information-sharing system. The system is envisaged to be integrated with a threat intelligence platform that would deliver selected information from the field. This would result in a real-time situational awareness that would strongly support decision-making and incident response. The most serious cyberattacks against the electric sector include data injection attacks against state estimation [5,6], DoS and DDoS [7], targeted attacks, coordinated attacks, hybrid attacks, and advanced persistent threats [8,9]. Additionally, ransomware campaigns have become a great danger to the sector in recent years [10–12]. EE-ISAC should support an informed defence against the cyberthreats.

This paper presents the results of a detailed analysis of the EE-ISAC's applicability properties based on the conceptual framework described in [1]. This applicability framework was formed by analysing the uptake of cybersecurity assessment methods by individual organisations. This paper brings the framework to a different setting, where multiple organisations are cooperating in cybersecurity. By investigating the applicability properties of the ISAC approach, this work contributes to assuring the broader adoption of cybersecurity cooperation. The recommendations offered by this analysis come at an important time during EE-ISAC's development, as their approach adapts to a changing regulatory and threat landscape. The study aimed at identifying the areas that require further development to improve the usefulness of the platform for energy sector participants. At the same time, studying a cybersecurity solution that has achieved a broader adoption provides a valuable insight into the applicability domain, exemplifying the proper fulfillment of the applicability requirements. This work also emphasises the importance of trustworthiness in the uptake and acceptance of methods and approaches.

The paper is organised as follows. In the next section, the related work that embraces two main fields, namely the methods' and solutions' applicability and the developments related to Information Sharing and Analysis Centres, is described. The EE-ISAC is introduced in Section 3, where the key objectives, stakeholders, and operational functioning of the organisation are described. This is followed by a detailed description of the applicability analysis that spans Sections 4–6. In Section 4, a general overview of the results, including a completed applicability control list, is provided. Section 5 is dedicated to the continuity of support-related applicability features. Section 6 focuses on the quality of documentation, provision of supporting tools, indication of target users, as well as solution evaluation and completeness. The complexity, usability, and acceptance properties are addressed in Section 7. The paper ends with concluding remarks. There, further areas of research and development are also demarcated.

2. Related Work

Two main research areas need to be considered in the analysis of relevant work: the domain of methods' and solutions' applicability and the developments related to Information Sharing and Analysis Centres.

2.1. Applicability

A systematic literature review revealed that methods' and solutions' applicability is a pioneering area [1]. Three studies that mentioned metrics or determinants in the context of applicability were identified. The studies focus on particular application domains. The research of Hong et al. [2] was devoted to graphical security models. After introducing a comprehensive taxonomy of the solutions, the authors discussed certain aspects related to their application. Namely, they identified the cybersecurity metrics most commonly utilised by the models and recognised the supporting tools that had been reported and made available to the public. Additionally, application domains were recognised. Lantow and Sandkuhl [3] investigated the applicability of ontology quality metrics to content ontology design patterns. The stability of the metrics' differentiating capabilities when applied to the new domain was verified. Moreover, the quality indicators obtained with the metrics were compared to the perceptions of quality provided by ontology engineers. The

study demonstrated that quality was an essential factor for the acceptance of technologies and solutions and the usability of products. Ling et al. [4] researched the use of information technologies among school educators in Malaysia. The Unified Theory of Acceptance and Use of Technology model (UTAUT) and the Technology Acceptance Model (TAM) were employed for that purpose. As a result of a comparative analysis of the frameworks, the UTAUT model was selected for analysing the situation in Malaysia.

A more general insight on applicability is provided in [1]. There, an applicability taxonomy and a questionnaire were introduced based on identified determinants and metrics. In the continuation of the research, the applicability of 32 cybersecurity assessment methods was evaluated [1]. The study evidenced that the methods' practical use in operational contexts was scarce. At the same time, the proposals were limited to pilots or demonstrators, hypothetical scenarios, or only basic configurations. The situation was explained by the methods' applicability properties, including the documentation detail, supporting tools, and time and effort indications.

2.2. Information Sharing and Analysis Centres

As far as the Information Sharing and Analysis Centres (ISACs)-related literature is concerned, Liu et al. [13] analysed the incentive issues associated with the membership of the Financial Services Information Sharing and Analysis Center (FS-ISAC). Based on a game-theoretic model, the authors devised improvements to the membership policies to evade the problem of passive, advantage-taking participation and a lack of information sharing. Additionally, Appan et al. [14] investigated the motivations for joining an ISAC. Their analyses focused on the Information Technology Information Sharing and Analysis Center (IT-ISAC) established by a group of IT enterprises. In this context, the impact of security information sharing was also studied [15]. The research exhibited the better financial performance of ISAC's participants in comparison to their industry peers. Mermoud et al. [16] employed the behavioural theory to investigate the relationships between human activities and the extent of information sharing. The authors conducted a survey among 424 members of the Swiss national ISAC, MELANI-net, of whom 262 responded. The quantitative research showed a positive association between CIS and the scale to which participants expected their information sharing to be rewarded in terms of career progression. At the same time, a negative association between operational costs and both the frequency and intensity of knowledge exchange was confirmed empirically. Leszczyna et al. [17] presented solutions proposed during the formation of the European Energy Information Sharing and Analysis Centre (EE-ISAC), namely a three-tier situation awareness network (SAN) and a dedicated, sectoral cyber incident information sharing platform (ISP), together with supporting mechanisms. From the nonscientific literature, the report of the European Union Agency for Cybersecurity (ENISA) [18] provides valuable insight. The study investigated the situation of ISACs in Europe by identifying the centres established in Europe, both international and national, and analysing their status. The collaboration models applied, as well as the challenges faced during set up and operation, were analysed. Based on the findings, recommendations aiming at strengthening the role of ISACs were formulated.

Other relevant research is related to cybersecurity information sharing and situational awareness and spans five main domains, i.e., the economic aspects of information sharing (IS), models and determinants of IS, data formats, supporting tools, and conceptual frameworks. In the area of the economic aspects of cybersecurity information sharing (CIS), Rashid et al. [19] analysed the CIS environment and interrelationships among stakeholders. Based on the outcome, they developed an economic model that allowed for determining the values created by exchanging cybersecurity knowledge as well as their distribution among participants. The research drew attention to finding a balance between information-provider commission to restitute their costs and the costs for end-users. Here, a sustainable business model plays an important role. Otherwise, the risk of CIS being suspended increases. In the paper, the authors provided a broader overview of the studies dedicated to

CIS. Yang et al. [20] employed the difference-in-differences approach to estimate the effect of the US Cybersecurity Information Sharing Act (CISA) on overall enterprise performance in the US. The results of all the analyses showed that large US cybersecurity companies are the primary beneficiaries of CISA. Tosh et al. [21] studied the benefits from information sharing based on their model of the CIS ecosystem as an evolutionary game between institutions. Economic models, including game-theoretical models, were applied to analyse incentives for information exchange and the effect of the exchange on cybersecurity expenditures [22–24]. Additionally, relationships between knowledge-sharing decisions and cybersecurity spendings were studied [25]. Regarding information exchange models and factors, incentives to share security data were analysed from several perspectives [26–28]. Additionally, the role of information exchange in cybersecurity strategies was determined using the game theory [29–31]. Guiding principles for cybersecurity knowledge exchange were determined by taking the healthcare sector as a reference [32].

Multiple standards and specifications have been developed to support the sharing of cybersecurity data [33]. These include the Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX), and Structured Threat Information Expression (STIX) [34–36], from which many newer proposals have been derived [34,36,37]. Additionally, various tools have been developed to facilitate cybersecurity knowledge sharing and situation awareness, including anonymisation mechanisms for information exchange [38] and vulnerability analysis frameworks [39]. Collaborative Intrusion Detection (CIDS) is a prospective methodology for detecting modern cyberattacks that has been studied already for more than ten years [40]. As a result, a privacy-preserving machine-learning-based CIDS for vehicular ad hoc networks (VANETs) [41], a CIDS for smart grids [42], a trust-based clustering support for deploying CIDS in wireless sensor networks [43], and a CIDS for Advanced Metering Infrastructure (AMI) [44] were proposed. Regarding operational IS or SA architectures, commercial or community-driven platforms such as AlienVault Open Threat Exchange (OTX), the Malware Information Sharing Project (MISP), and ThreatView's Cyber Threat and Reputation Intelligence were introduced. The scientific research has been focused on conceptual models or methodologies [45–50]. More practical proposals include a platform for the detection of suspicious hosts in large computing environments [51], a system for analysing event logs collected from various distributed network locations [52], and a framework for the integration of heterogeneous data from multiple architectural layers and domains [53].

A systematic review of information sharing in the cybersecurity domain was carried out by Pala and Zhuang [54]. During an iterative literature search process, they identified 82 papers relevant to the topic. According to the authors, the research falls into four categories: technical/conceptual designs of information-sharing platforms and supportive tools, legal frameworks, game-theoretical models of information-sharing contexts, and other analytical models to analyse the behaviours of participants.

2.3. Summary

The research shows that CIS and SA can form a potent weapon against cyberthreats faced by the energy sector nowadays. The literature delivers many ideas that could be employed during the development of operational solutions. At the same time, the majority of proposals are still in the conceptual phase. Till now, situational awareness and information exchange have been addressed distinctly. However, to obtain the full benefit of these areas they need to be integrated [50]. The EE-ISAC described in this paper supports such a joint approach. The solutions' applicability is a pioneering research domain. Only a few studies relevant to metrics and determinants in the applicability context have been conducted, and they are focused on particular application areas. The detailed analysis of the applicability presented in this paper is based on the most recent developments in the area. It aims at providing further insight into applicability success factors in general as well as demarcating the improvement directions for the EE-ISAC.

3. EE-ISAC—The Objectives, Stakeholders, Operational Functioning

Information Sharing and Analysis Centres (ISACs) are associations designated for sector-specific information exchange on cybersecurity incidents [55]. The European Energy ISAC (EE-ISAC) attracts members from utilities, suppliers to utilities, cybersecurity solution providers, and academia and research organisations. With an uncertain picture of evolving threats, the sharing of the latest cybersecurity knowledge among sector stakeholders can inform and improve decisions and responses.

The original key aims to be fostered by the EE-ISAC were:

- Sector-specific intelligence across the energy value chain;
- The engagement of a variety of sector stakeholders;
- Access to a broad network of organizations;
- A proactive and trust-based sharing community;
- Enhancing organizational resilience and preparedness.

Delivering on each of these aims has set the foundations of the EE-ISAC during its first 5 years. The operational functioning of the EE-ISAC is now going through an adjustment due to the evolving cybersecurity regulations and new cross-border arrangements coming under the Network Code for Cyber Security (NCCS). The EE-ISAC board are looking to formalise the ISAC's role within the new procedures and regulations. The following analysis using the applicability framework intends to steer towards a more practical way forward for the EE-ISAC within the current landscape.

The EU Cybersecurity Strategy [56] recognises the shared responsibility involved in ensuring security and the need for a coordinated response among relevant actors. It emphasises effective cooperation between the public and private sectors as being crucial due to a government's duty to protect critical infrastructure that exists within the private sector [56]. The regulatory activity underpinning the cybersecurity of essential services is dynamic, with multiple actors participating. It requires coordination across a distributed accountability and effective communication between actors to improve their capacity to make more informed decisions while protecting our infrastructure and responding to events [57]. The concept of cybersecurity as a shared mission and the reality that "no single management entity has control over the whole" [58] has encouraged partnerships such as ISACs to form. A gradual building of long-term relationships, starting small and cooperating in a network of trust, allows an understanding of shared risks and supports continuous learning and adaptation to the latest situation. The formation of the EE-ISAC has fostered a unique environment of trust for information sharing and collaborative opportunities, acting as a significant enabler of improved resilience for the energy sector. Professional loyalty to the cause with a basis of moral principles brings a subtle power of commitment to such partnerships that goes beyond self-interest. The association has progressed, often through voluntary contribution, and by going beyond immediate results without specifying outcomes [59].

4. Detailed Applicability Analysis

The EE-ISAC has been successfully adopted by multiple organisations. In this context, analysing its applicability characteristics can provide valuable insight into the factors that determined the successful adoption. Additionally, it can help in finding where additional effort needs to be allocated. The assessment was based on the control list developed during the research on the applicability of new methods and tools [1,60,61]. The list is provided in Table 1. There, the answers to the control questions are also presented. In the future, the applicability analysis will be extended with external evaluations, e.g., based on the applicability questionnaire.

Table 1. Applicability control list. The symbol ☑ depicts a completely addressed control question. ▣ indicates an area that has been partially covered.

A. Continuity of Support		
A01. Will your solution's continuity be actively maintained with frequent events organised and broad training provided?	Yes ☑	No ☐
A02. Will the solution be improved and are new versions' releases planned?	Yes ☑	No ☐
A03. Have you built a large community of supporters?	Yes ☑	No ☐
A04. Have you developed a funding model that assures the continuity of support?	Yes ☑	No ☐
B. Documentation, Tools, Target Users, Method Evaluation, and Completeness		
B01. Have you provided detailed documentation of the solution?	Yes ☑	No ☐
B02. Have you developed and shared tools that support the use of the solution?	Yes ☑	No ☐
B03. Have you indicated the target users of the solution?	Yes ☑	No ☐
B04. Have you tried to minimise the level of skills required to operate the solution?	Yes ☑	No ☐
B05. Have you evaluated the effectiveness and efficiency of the solution and published information about that?	Yes ▣	No ☐
B06. Have you assured the completeness of results obtained with the solution?	Yes ▣	No ☐
C. Complexity, Usability, Acceptance Properties		
C01. Have you tried to reduce the difficulty of understanding the solution?	Yes ☑	No ☐
C02. Have you tried to reduce the difficulty of describing the solution?	Yes ☑	No ☐
C03. Have you tried to reduce the difficulty of (re)creating the solution?	Yes ☑	No ☐
C04. Have you assured that the solution approaches the addressed problem with high precision?	Yes ☑	No ☐
C05. Have you assured that precise results are obtained with the solution?	Yes ☑	No ☐
C06. Have you assured that the solution comprehensively tackles the entire addressed problem?	Yes ☑	No ☐
C07. Have you evaluated the subjective opinions of experts regarding their impressions on using the solution?	Yes ☑	No ☐
C08. Have you evaluated users' subjective perception of the likelihood that using the solution will increase their performance within a specific context?	Yes ☐	No ☑

This applicability analysis is applied in detail to the cybersecurity situation awareness of faults and attacks in the energy sector in order to identify progress and improvements for the EE-ISAC as a practical cybersecurity solution for the energy sector. This is placed within an evolving regulatory landscape that is looking to improve cybersecurity levels across the whole energy sector. Furthermore, ISACs are seen as an important tool to achieve collaboration, interworking, and sharing across private entities that contribute to the cybersecurity level of essential services. In the following sections (Sections 4–6), detailed descriptions of the applicability areas indicated in the control list (Table 1) are provided.

5. Continuity of Support

The EE-ISAC has established a rhythm of continuity by supporting its membership with regular plenaries and webinars. In addition, regular touchpoints for each of the technical working groups have also maintained a momentum of progress in specific topic areas. The ISAC concept continues to be supported by the European Commission and the European Union Agency for Cybersecurity (ENISA), which encourages ISAC membership and facilitates interaction between cross-sector ISACs.

5.1. Events, Training (A01)

A previous study of interorganisational partnerships solving problems together and transferring best practices has shown that knowledge sharing is nurtured by different perspectives, relative trust, and by sharing collective memories. Expertise is shared through telling the story of previous events and happenings [62]. There has been an increasing willingness over time, especially amongst the established utility members, to bring their latest operational experiences of dealing with security events to plenaries for sharing and discussion. This has created "a cybersecurity heartland" for the energy sector that formed gradually through partnership, mutual interest, and sharing common responsibilities [63]. A gradual building of trust and an openness to share evolved, and the confidential information-sharing session, as a regular slot that was increasingly well-contributed-to, became a foundational part of the culture of the EE-ISAC. The expectation to bring experiences to share became a behavioural norm in this culture of voluntary participation. More importantly, the themes of these information-sharing sessions emphasise applicability to power system scenarios and offer a dialogue on cybersecurity issues within the context of operational technologies and energy-system dynamics. This created value for member organisations that were integrating IT, Operational Technology (OT), and cybersecurity.

Forming interorganisation groups, through having a shared focus and identity creates trust and builds stability. Several technical working groups invited contributions from different competencies to engage in specific information-sharing activities. The topics and projects that progressed were dependent upon member interest and availability to contribute. This has enabled knowledge transfer by bringing different perspectives and experiences and different points of view to the table, learning how different companies are responding to similar situations [62]. The projects performed by EE-ISAC Technical Working Groups are summarised in Table 2. There, the relevance of a project to applicability control areas is also illustrated.

Education and awareness are facilitated by webinars and round table working groups, where members decide and vote for topics and themes of interest. Meaningful webinars share knowledge, create opportunities for information sharing and cooperation, and raise awareness on important issues. This working group has evolved to provide more interactive sessions, encouraging live discussion on topics such as:

- Building a Security Operations Centre (SOC) for utilities;
- Maturity models;
- Securing the human element;
- Discovering and defending against vulnerabilities.

5.2. Improvements (A02)

A review of the EE-ISAC was carried out to identify improvements and is detailed in Section 6.5. Improvements have also been in progress through the Empowering ISACs project. This is a facilitation management project funded by the EU to support the maturity of existing and emerging ISACs in Europe, lasting three years until December 2022. During its first phase, the project collected the needs of existing maturing ISAC organisations and supported the set-up of new ISACs. The second phase investigated ISAC needs for platforms and tools to gather future requirements. The third and final workstream is related to the provision of legal support to existing and emerging ISACs. EE-ISAC members have provided input to this project on a regular basis. Following this three-year project, ENISA will host and maintain the tools that are developed.

There will be a common IT platform for ISAC enablement, which is a standard tool developed for all ISACs. The light platform contains a public domain and opensource applications with basic functionality, whereas the full platform contains enterprise-grade Software as a Service (SaaS) applications, for which a paid subscription is required. The design of the tool was intended to encourage information sharing within a single organization to mainly share information and analysis among ISAC members, but the EE-ISAC has a requirement for dedicated channels for sharing with external peers and international

partners, so the possibility to further exchange information with third parties will need to be taken into consideration in a future version. The EE-ISAC has contributed their knowledge and experience to this facilities-management project to assist newer ISACs. The EE-ISAC will benefit from the new tools after submitting their requirements to the design process. The first release will include a Malware Information Sharing Platform (MISP), a document-management system, and communication modules. Onboarding is underway to utilise the new platform solution in parallel with existing tools for a trial period.

Table 2. Projects performed by EE-ISAC Technical Working Groups and their relevance to applicability control areas.

Project	Activity	Applicability Control Area
Building a network of trust	A cultural foundation of the ISAC. Confidential information sharing. Regular slot at member plenary meetings. Sharing experiences on specific topics.	A01, A02, A03, B01, B02, B03, B06, C01, C02, C03, C04, C05, C07.
Deep-dive into system requirements	Investigation of platform use cases. Future system requirements of the ISAC.	A02, A04, B02, B03, B04, B05, B06, C01, C02, C03, C04, C05, C06, C07.
MISP instance	Curating threat intelligence for OT community. Building threat intelligence for energy context.	A01, A02, B02, B03, B06, C04, C05, C06, C07.
Risk management for digitalized energy Systems	Combine outputs of 3 academic cybersecurity projects on risk management. To inspire practical applications by energy operators.	A03, B01, B02, B03, B04, B05, C01, C02, C06.
Threat intelligence	Combine experience into a living document on threat intelligence management. To share new approaches over time.	A01, A02, B01, B02, B03, B06, C04, C05, C06, C07.
Incident response white paper	A collaboration of members and invited experts. Shared knowledge and experience of incident response tailored to the energy sector.	A01, A02, B01, B02, B03, B06, C04, C05, C06, C07.
Public–private cooperation in energy cybersecurity	A session between the EE-ISAC and the NIS Cooperation Group. Experiences of implementing the NIS directive shared with national authorities.	A01, A03, B01, B05, B06, C01, C06, C07.
EU advocacy working group	A voice for the energy sector. Provides energy-sector-specific feedback, anonymised where necessary, to the regulation and policy arena.	A01, A03, B01, B05, B06, C01, C06, C07.
Information sharing with international partners	Facilitating a regular opportunity for energy-sector sharing with international partners.	A01, A02, A03, B02, B05, C01, C02, C06, C07.

5.3. Building Community (A03)

A focus on having utility representatives at the core of activities brings an emphasis on OT and the energy sector in the operational functioning of the ISAC. Building and maintaining trusting relationships amongst EE-ISAC members is crucial to encourage information sharing and collaborations. This was achieved by starting small to establish a sharing culture and growing at a steady pace. Members are required to specify two representatives from their organisation who must be approved by existing members. All representatives sign confidentiality agreements to interact with the sharing platforms and attend meetings and events, without substitution. This provides consistency in the network

to build trust and a feeling of shared responsibility. As a result, close working relationships have gradually been established.

A community of partners has also been established with ISACs in other sectors and countries. Engagement is now in place with American and Japanese E-ISACs, including monthly discussions to plan the next steps for the collaboration and quarterly meetings for trilateral information sharing. This continuous support for the trilateral partnership has encouraged regular contribution within a Memorandum of Understanding (MOU).

5.4. Funding Model (A04)

The EE-ISAC is currently funded through membership fees, paid annually by member organisations. In some cases, an in-kind contribution is given instead, such as for academic members. Participation in ISACs is being incentivised within EU funding mechanisms. Membership of, and participation in, an ISAC is seen as favourable to encourage the sharing of knowledge and experience from implementing cybersecurity improvements [64]. This mechanism has indirectly contributed to funding by encouraging new members to join. In addition, the EE-ISAC has also benefited from the EU funded Empowering ISACs project developing new tools to support ISACs. However, it can sometimes be challenging to meet expectations with international partners where they are additionally funded and supported by large teams of analysts.

The EE-ISAC technical working groups are largely dependent on voluntary contributions from the members, and there are limits to how much time and effort each member can give to the network. Additional funding will be required to mature the ISAC; however, time and resources are needed to be able to participate in funding applications. Unfortunately, the ISAC had to reduce participation in funding calls due to not having the resources to follow through with the actions. Maintaining the ISAC with an appropriate balance of members and ensuring it is adequately funded and resourced to fulfil its role is crucial. The continuous management of EE-ISAC working groups, instead of the current ad hoc contributions from willing members, is also paramount to guide efforts with regular progress towards achieving the aims of technical working groups.

6. Documentation, Tools, Target Users, Solution Evaluation, and Completeness

Providing detailed documentation, indicating target users, and evaluating the quality of a solution are important determinants of its applicability [60]. This section presents how these areas are addressed by the EE-ISAC.

6.1. Documentation (B01)

The EE-ISAC association has documented and updated strategic plans each year and its structure and procedures are defined in a terms of reference document. The documentation produced by the technical working groups has demonstrated the synthesis of skills and expertise within the ISAC. Experiences in incident response for an OT context were gathered from a group of ISAC members and experts in the field to create content to share within and beyond the membership, especially for smaller utilities that may have fewer resources for incident response and do not have the chance to join the ISAC [65].

A white paper on risk management for digitalized energy systems was produced by academic members to bring together contributions from three recent cybersecurity projects that all included a component of risk management [66]. Feedback from the wider membership was invited to help shape this work to be more applicable to utility requirements and to inspire some practical applications. The threat intelligence working group provided a white paper on threat intelligence management which has become a living document to share new approaches over time [67]. EE-ISAC members are also invited to contribute to ENISA's annual threat landscape report for the energy sector [68].

6.2. Supporting Tools (B02)

A core working group essential to the ISAC was focused on building threat intelligence tailored for the energy context. An information-sharing system was proposed to facilitate threat intelligence and a technical pilot arranged for the curation of threat intelligence for the OT community. The vast quantity of information provided in threat intelligence feeds needs to be customised and translated into useful, actionable intelligence, especially to provide specifics for the energy sector and critical infrastructure operators.

The core threat intelligence working group was made up of 70% utility members and was responsible for checking the application and features, confirming the information feeds going into MISP, and agreeing on procedures and criteria before the platform access was opened up to further interested members. Eventually, 55 threat intelligence sources were integrated into MISP and a vetting process for the integration of new intelligence information had been defined by the core team. A live demonstration of the platform was given at a plenary session, including the use of the tool to share information and to perform better analysis of threat trends to help operators identify false positives and have a more structured collection of events. There is now a transition underway to the new platform designed by the Empowering EU-ISACs project, as described in Section 5.2. Simultaneously, the Vmoso knowledge sharing platform is utilised by EE-ISAC members [69].

6.3. Target Users (B03)

The target users of the EE-ISAC are visibly indicated on the website. Central to the EE-ISAC's role has been to develop a cybersecurity information hub and communications channel for the energy sector in Europe, facilitating the sharing of best practices and the dissemination of mitigation strategies. It has been necessary to maintain a strong presence of utility organisations in the membership and management of the ISAC. Mechanisms and incentives have been put in place to ensure a balance of participants in the EE-ISAC and encourage an approach that is tailored towards the needs of energy utilities and the context of operating a power system. It is also stipulated that the leadership team always has three out of five board members coming from utility organisations. On some occasions, it has been necessary to redress the balance of members by pausing membership requests from nonutility organisations until more utilities were recruited.

Attention was given to partnering with expertise to bring value to the members and the energy sector. Both European and International links were established in the early stages of building the ISAC, setting a foundation of partnership to enhance incident analysis, threat intelligence, and collaborative opportunities for the energy sector. Twenty-eight organisations have signed the membership, including representatives of utilities, vendors, public bodies, and academia and research labs; mutual agreements have been signed with nine partners; and ten working groups have been established for specific actions.

Following the Directive on Network and Information Security (NIS) and with more information exchange coming under the revised NIS2 regulatory obligation, members may become less interested in participating in further sharing within the EE-ISAC. This may influence the EE-ISAC's voluntary sharing activities away from incidents and towards exchange regarding solutions. The essence of an ISAC is its core of contributors, so it is essential at this time to set a strategic direction for the ISAC and attract relevant engagement. Going forward, due to the broader coverage of NIS2 to include more entities and engage wider preparations, it will likely be necessary to review the spread of members. For example, actors in the energy system that do not come under NIS2 or NCCS arrangements, such as Small or Medium Enterprises (SMEs), may benefit from becoming involved in ISAC information sharing regarding incidents and threats and contributing to situation awareness. This adaption and realignment of the EE-ISAC is further discussed in Section 7.7.

6.4. Required Level of Skills (B04)

The operational functioning of the ISAC with utilities at the centre continuously educates members in the area of OT and improves their understanding of the Industrial

Control System (ICS) context. For the use of ISAC tools, training was provided to members upon the introduction of the sharing platform and after new releases. Training for the MISP platform is now being offered by the Empowering ISACs project. With the upcoming transition to a new platform, key use cases will be presented to the ISAC community.

Appropriate skillsets are invited into working groups as required, for example, the threat intelligence team required skilled members to agree on which intelligence feeds to utilise, as described in Section 6.2. The incident-response working group actively sought appropriate skillsets from inside and outside the ISAC membership to gather the necessary expertise for an OT context, as described in Section 6.1.

In the future, it may become necessary to share relevant experience with new entities as the risk picture changes and new entities are identified as essential or important under NIS2 or the NCCS. Additionally, information sharing with new countries entering the continental synchronous grid area may be required. To achieve a wider situation awareness, along with a broad and deep adoption of consequence-focused cybersecurity, will require a large cadre of experience to bring together the necessary engagements and create a more inherently secure energy system [70].

6.5. Effectiveness and Efficiency (B05)

An interactive online plenary during 2020 was designed to reflect on the EE-ISAC's mission statement and discuss the next steps to undertake in the future. Members had appreciated the chance to cooperate beyond their individual organisations. The connections made between utility members were found to be a supportive group during challenging situations. The wider membership had benefitted from the core group of utility members giving them a closer understanding of the needs and requirements of energy operators. The member evaluation of the EE-ISAC's progress in Figure 1 shows the emphasis given to marketing and developing partnerships. Contrastingly, the analysis and best practice development and platform activity are still developing. Progressing these different aspects of the ISAC was influenced by the leanings of the most active participants. The availability of technical skills to support the ISAC on a voluntary basis came in fits and starts around other commitments when a member saw a possibility for the ISAC and gave some extra effort to lead or contribute to a technical working group.

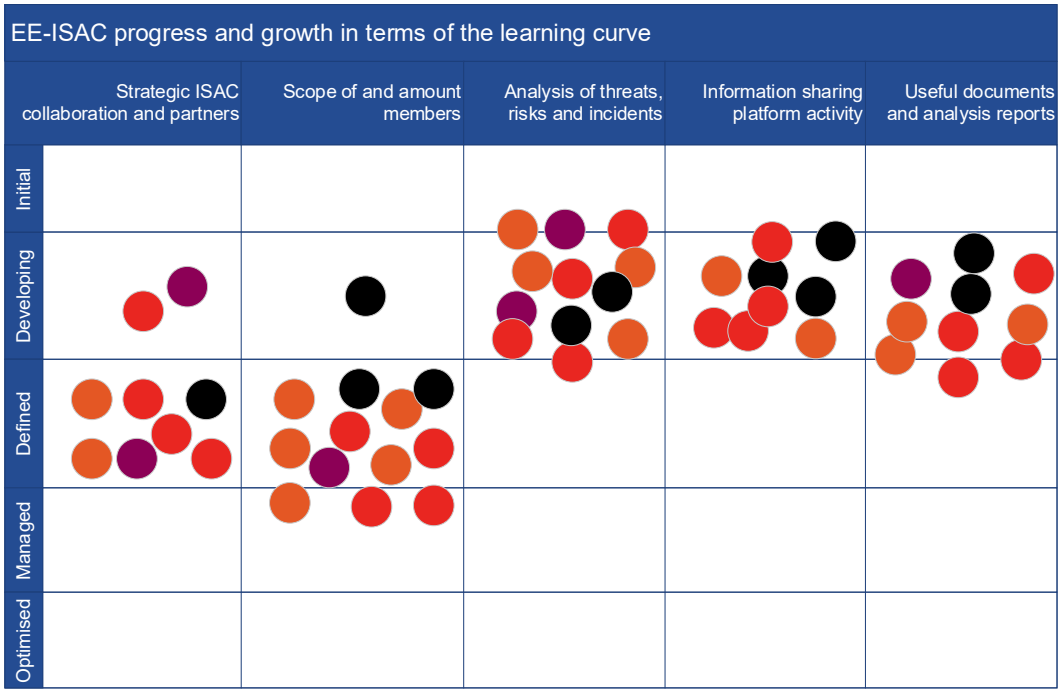

Figure 1. Progress of EE-ISAC development.

Figure 1 shows how the members perceive the current status of the EE-ISAC and its activities by using a rating scale in which the 'Initial' phase corresponds to stage one of developing the ISAC and the 'Optimized' phase to stage five. Each circle is a 'vote' or response from a member, showing their opinion on the development stage reached by the ISAC. Overall, the EE-ISAC's members perceive the growth of the EE-ISAC to have moved forward towards Developing/Defined levels of maturity. The human aspect is well established, with members and partners setting a strong foundation for the network of trust, while the sharing and analysis activities are still developing.

The feedback on working groups exposed the gap in the technical leadership of the ISAC due to limited funding and dependency on in-kind contributions. The foundation of trusted information sharing has formed well, especially in regular meetings. However, the analysis centre is in the early stages and would require funding to take it further, especially to match the teams of analysts in their partner ISACs in the US and Japan.

For the future of the ISAC, members emphasised the need for cooperation beyond their organisations and mutual support for members and the potential for the ISAC to facilitate public–private cooperation. Members were particularly interested in protecting the energy supply chain and understanding supply chain dependencies. They expressed ambition for their MISP project to become the official MISP platform for the energy sector, and the potential for a Security Operations Centre (SOC) network among the members. They suggested progressing towards the real-time monitoring of threats and providing an early warning function. There was even a desire to contribute to coordinating crisis management for the energy sector, especially to add energy-specific assistance to the role of the current CERT network. They also saw a need for mapping cross-border dependencies and for cross-sector collaboration on threat intelligence.

In this context, the following activities play an important role:

- Regular assessments of the performance of the EE-ISAC in terms of its contribution to operational, regulatory, and business aspects of cybersecurity;
- Periodic stakeholder reviews to keep on track with the goals of the ISAC;
- Gathering evidence that the EE-ISAC has assisted cybersecurity improvements across the entire energy system and synchronous grid area;
- Assisting businesses in improving their cyber performance and achieving regulatory requirements.

6.6. Assuring Completeness of Results Obtained by the ISAC (B06)

The EE-ISAC has been used as an example ISAC for other sectors, and the learning and experience of the EE-ISAC has informed the development of newer ISACs. The foundation of trusted information sharing has formed well. To assure the completeness of results from the ISAC, the analysis centre aspect would benefit from further development. Understanding the wider engineering solution of power systems could offer more predictive insight and actionable guidance to the energy sector. Further efforts to assure a more thorough contribution from the ISAC are suggested below.

- *Providing more actionable threat intelligence than utilities currently have access to.* Progress the MISP project towards the real-time monitoring and analysis of threats and the provision of an early warning function. To facilitate more proactive sharing, the association's culture of trusted sharing could be progressed further to take actions to help each other, such as with early indication and formulating guidance from joint experience, tailoring threat intelligence to the energy sector.
- *Working towards more effectively utilising collaborations with the entire network of partners, including other ISACs and cross-sector ISACs, to improve and integrate threat intelligence.* In agreement with partners, there should be some sharing of Indicators of Compromise (IoC) and general information on the targeting of energy-sector-relevant equipment or supply chains. Facilitating faster dissemination of new information to assist utility preparedness, e.g., IoC analysis or malware reverse engineering.

- *Contributing to a more holistic understanding of risks by providing sector knowledge on the potential impact of technology changes and system differences.* For instance, the consequences of the cybersecurity level of smaller and more distributed entities in a more complex and interconnected system, such as EV charge-point providers or the aggregated effects of smaller energy operators, can be considered. Additionally, sector experience to attend to potential gaps in NIS implementation or NCCS application can be offered. For example, its application to different entities, where the potential impact on the system rather than the size of the entity or customer base may be more relevant.
- *Exploring the potential for a Security Operations Centre (SOC) network among EE-ISAC members for the energy sector.* This is particularly pressing in light of the NCCS requiring grid entities to have access to SOC capabilities. Relevant activities include sharing learning from cybersecurity events or ensuring the appropriate dissemination of best practices, lessons learned, and post-incident recommendations.
- *Assuring completeness in terms of improving the level of cybersecurity more widely across the sector will benefit from diverse and relevant participation in the ISAC.* Work is in progress to extend the membership to the most relevant partners for a more complete approach, as outlined in Section 6.3.

7. Complexity, Usability, Acceptance Properties

This section provides details on the complexity, usability, and acceptance properties of the EE-ISAC's applicability.

7.1. Reducing the Difficulty of Understanding the ISAC Approach (C01)

The breadth of membership is improving the understanding and awareness of energy cybersecurity by bringing together diverse skillsets. Solution providers bring extensive knowledge in cybersecurity and utilities share operational experiences, and together this is building a situational awareness that is assisting the integration of cybersecurity into the practice of managing energy systems. This integrates the understanding of both faults and attacks, the operational and cybersecurity aspects of electricity networks that are now dependent on their digitalised monitoring and control capability.

7.2. Reducing the Difficulty of Describing the ISAC Approach (C02)

Each member organisation commits to a Terms of Reference (ToR) that defines the rules for information exchange and includes a confidentiality agreement on the nondisclosure of information that is classified by a Traffic Light Protocol (TLP). White papers have been produced to describe and present collaborative outputs from technical working groups. The overall ISAC approach has also been extensively described by the Empowering ISAC project to support new ISACs [71].

7.3. Reducing the Difficulty of (Re)Creation of the ISAC Approach (C03)

The formation of membership with an emphasis on energy operators adapts all ISAC activities to the energy context with an awareness of the functions and services being protected. Meeting topics and discussions relate to energy systems, for example, applying cybersecurity to electrical substations or in-home smart devices.

7.4. Level of Precision in Approaching the Problem by the ISAC (C04)

EE-ISAC members have participated in the development of a Network Code on Cybersecurity (NCCS) by a collaboration of European Transmission System Operators (TSOs) and European Distribution System Operators (E.DSO), led by the European Association for the cooperation of TSOs for electricity (ENTSO-E). Being involved from the outset, the EE-ISAC continues to contribute to reviewing these new arrangements. This NCCS specifies a framework for managing the cybersecurity aspect of cross-border electricity flows. Similar to the NIS Directive, it aims to provide a common cybersecurity level across the grid participants of the continental synchronous area spanning 28 countries, operated

by the ENTSO-E. Participants in this synchronous area may impact their neighbours during a cybersecurity event if the consequences affect power flows on the system. The NCCS for cybersecurity is an opportunity to create a translation of NIS for the energy sector, particularly with regard to cross-border impact. The ENTSO-E, E.DSO, and national authorities will create a list of cybersecurity principles that electricity entities must meet.

There was a concern during the NCCS drafting process that the NCCS seems to overlap with or duplicate NIS. The information-sharing mechanisms proposed by government in NIS2 use national borders as their framework, whereas the actual operational and technical boundaries differ. The operational boundaries of energy companies can be within a member state or operate across borders for larger organisations. The technical boundaries correspond to the synchronous AC grid area, which is electrically tied at the same frequency, where power supply and demand is balanced in real time. The NCCS defines the operational and technical cybersecurity requirements alongside the national expectations laid down by NIS2. By involving National Competent Authorities (NCAs) in the process of developing the NCCS, there is an opportunity to reconcile different national approaches to implementing NIS to include or enhance national NIS obligations and ensure sector-specific cybersecurity principles appropriate for the cross-border dependencies that arise within the electricity system.

Alongside the network of Computer Security Incident Response Teams (CSIRT) between member states, established by the NIS directive, it is recommended that grid entities establish a SOC or access SOC capabilities through a Managed Security Service Provider (MSSP) to ensure incident response capability at the entity level, unless the CSIRT at the national level is engaged to handle incidents (see Figure 2) [72].

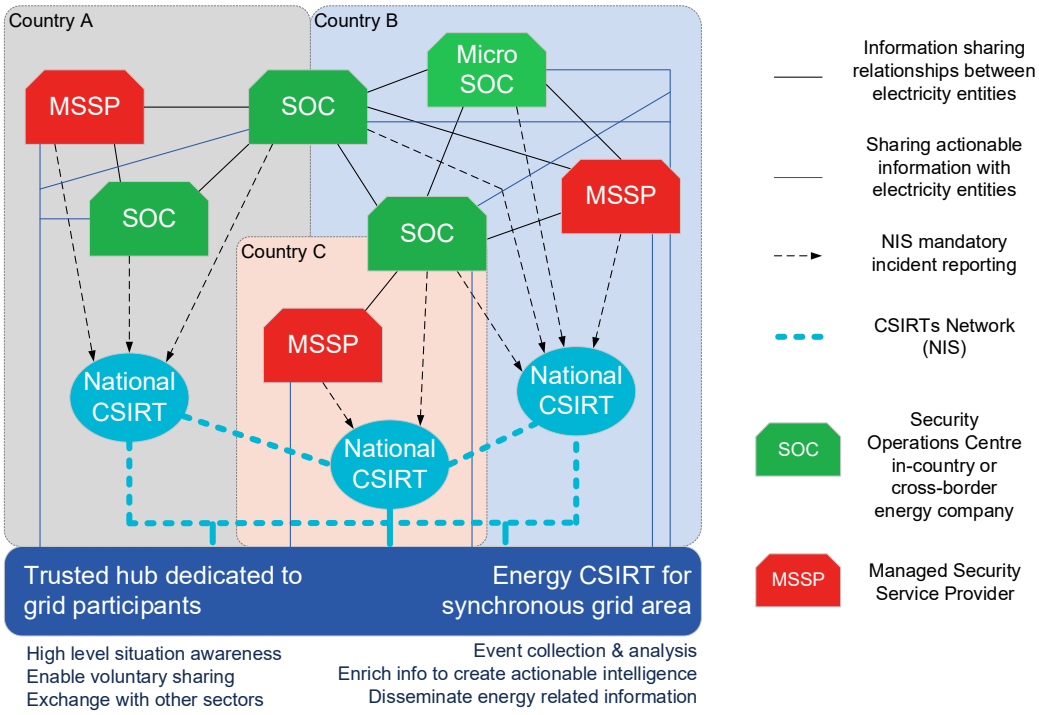

Figure 2. Information sharing between electricity entities [72,73].

The CSIRT network established by NIS is likely to prioritise dissemination across sectors nationally before attending to international dissemination. Rapid sharing is important to minimise cascading effects in a connected grid. Grid entities must be able to alert other electricity entities and respond rapidly themselves when alerted. Essential entities with the potential to impact cross-border flows in the synchronised area ought to have access to a combined view of relevant information and incidents. Currently, no entity has the

whole picture of cross-border risks [74]. Providing a combined view to such entities in an anonymised and secure manner could be a future role for the EE-ISAC in collaboration with the ENTSO-E and E.DSO. High-level situation awareness is needed to build a perspective on what the energy grid is experiencing and what the digital monitoring and control capability is experiencing. Guidance and decision support on cross-border risks from this higher strategic level will be important to aid preparations, in addition to on-the-ground reporting from individual grid entities. The essential building blocks of this combined view will be the electricity entities who contribute to cross-border risks, all having monitoring, detection, and response capabilities in place.

The drafting team for the network code have recognised the essential need for a high trust setting, giving the confidence to share timely information among grid participants to reduce the exposure of the grid to known and exploited attacks. This voluntary sharing among electricity entities in the synchronous grid area is included in Figure 2. It is suggested that a subgroup within the EE-ISAC could offer a trusted hub dedicated to grid participants to provide the proposed energy CSIRT in the European landscape [73].

Further to the strategic direction provided by the NCCS, the EE-ISAC can assist at the operational and technical levels, interpreting events together. The trusted network in the EE-ISAC provides a network of support for utilities that includes researchers and solution providers. EE-ISAC activities could contribute to assisting energy-sector companies with meeting their obligations under NIS2 and the NCCS. A more precise definition of the EE-ISAC's role within these new arrangements will be needed to achieve an improved cybersecurity level across the synchronous grid area.

7.5. Level of Precision in Obtaining Results from the ISAC (C05)

Extending situation awareness capability to consider both faults and attacks, implying the integration of cybersecurity activity with operational consequences, could help to prioritise response actions to what is really needed. The regulatory approach through NIS2 and the NCCS attempts to connect cybersecurity levels with an impact on energy supply or an impact on cross-border electricity flows. These arrangements encourage better preparation for cyber attacks and oblige the notification of incidents if those attacks cause (or nearly cause) a fault within the system or affect the service provided.

Being able to categorise an incident to notify and elicit an appropriate response requires a clear understanding of the impact on the system. Understanding if a cybersecurity event will lead to an operational incident requires the capability to determine the technical consequence and the business impact from the Indicators of Compromise (IoC). A cyber event needs to be translated to a potential physical event to assess the impact on essential services [75]. Likewise, faults appearing in a cyber–physical system could be triggered by a physical or cyber event. For example, an effect on system dynamics could have been caused by a physical line fault or by a compromised device [76]. The consideration of both faults and attacks is necessary for building situation awareness. Creating more actionable threat intelligence is a goal of the EE-ISAC threat-intelligence working group to meet their utility member needs.

7.6. Comprehensive Approach to Fully Address the Problem (C06)

Relevant OT experiences and challenges are brought to the table for discussion. Members have gained a better awareness of energy cybersecurity through more extensive information sharing and improved threat intelligence. The EE-ISAC acts as a voice for the energy sector. An example of this was to provide feedback on the experiences and discuss the challenges related to implementing the NIS directive with national authorities via the NIS cooperation group's energy workstream. An anonymous space was created to gather the NIS experiences of energy operators, and the EE-ISAC combined and presented operators' feedback, thus achieving the benefits of collaboration while also addressing the need to protect information [77]. This session between the EE-ISAC and the NIS cooperation group was noted by ENISA as the first public–private cooperation in energy

cybersecurity. In this way, the EE-ISAC consolidated its presence as a reference point in European critical infrastructure protection. A requirement for the NIS Cooperation Group to organise "regular joint meetings with relevant private interested parties from across the Union to discuss activities carried out by the Group and gather input on emerging policy challenges" [78] has since been written into Article 12 of the NIS2 proposal.

To further address the entirety of the cybersecurity problem, the EE-ISAC could engage with interdependent sectors, such as the telecoms sector, to ensure cybersecurity across end-to-end solutions. There may also be scope to facilitate progress in protecting the energy supply chain and understanding supply chain dependencies by fostering a closer understanding and alignment with vendors and solution providers and communicating the common cybersecurity needs and requirements of energy utilities.

7.7. Evaluation of Expert Opinion on the Utility of ISAC (C07)

Member impressions of the ISAC were evaluated, as described in Section 6.5. Feedback on utilising the sharing platforms was also elicited during requirements collection for the Empowering ISACs project, as an input for future tool development. The upcoming training on newly designed platforms will be an opportune moment to again review the needs of members in terms of the utility of EE-ISAC platforms.

The overall EE-ISAC approach may need to adapt in the light of new regulatory measures, such as the NIS2 proposal to promote effective information sharing and introduce additional cross-border responsibilities for member states, as presented in Table 3. While the EE-ISAC was founded on voluntary information sharing, the regulatory landscape is introducing obligatory sharing. Participation in information sharing between companies is now included in entities' notification responsibilities to Competent Authorities (CA) under NIS2, citing the EE-ISAC as an example of "already existing capability and well-established frameworks" [78].

Table 3. Information-sharing models according to the revised directive on Network and Information Security [78,79].

Information-Sharing Model	Description
Enterprises–enterprises	Article 26 requires companies to exchange relevant cybersecurity information between themselves within trusted communities; NIS2 now obliges companies to join an ISAC and report their participation to their national authority.
Enterprises–national authorities	Article 20 requires companies to report incidents and also to report threats that could have resulted in an incident, i.e., near misses, to their CA.
National authorities–national authorities	Article 11 requires cooperation between CAs, CSIRTs, and a Single Point of Contact (SPOC) within each member state, in providing information on risks, threats, and incidents.
Member states–member states	Cross-border impact of reported incidents and near misses is assessed by the national authority, and the information is passed to other member states and ENISA, as required. SPOCs provide monthly incident summary reports to ENISA. National CSIRTs are to communicate with the CSIRT network where a disclosed vulnerability impacts products and services provided across borders; ENISA will maintain a vulnerability registry, providing access to interested parties.

These formal structures for cooperation need to be translated into practical support for infrastructure operators, who require timely actionable threat information to prepare and respond rapidly to incidents. The cross-country exchange of information, from operators to national authorities and back to other national authorities, has so far not been running smoothly. Notification obligations under NIS have required energy operators to share information with their authorities, but it is often perceived that assistance from government agencies has not been reciprocal [80]. On receiving a notification of incidents, attention needs to be focused on minimising their impact. Relevant information must be gathered and analysed by the national CA. Energy operators need an appropriate channel in place for the CA to rapidly forward such relevant information to assist operators with the rapid closure of vulnerabilities. A two-way process is most advisable, by requesting that national authorities also report to operators or sectoral ISACs on incidents, rather than only the company being obliged to report to authorities. The ISACs are in a position to enrich this information, making it sector-specific, to provide more actionable information to their utility members. The reporting of "near misses" and disruptions threatening their infrastructures to national CAs should also be directed to other operators in Europe of such attempts of attack, i.e., sharing indicators of compromise, so they can promptly verify whether they are also susceptible to such risks and initiate suitable countermeasures. Additionally, ISACs could play a fundamental role in the analysis at the international level of potential weaknesses and early indicators of threats that are meaningful for ex post incident analysis and reporting [81].

Article 13 establishes the CSIRT network "to contribute to developing confidence and trust between the Member States. It intends "to promote swift and effective operational cooperation" [78]. As the CSIRT network exchanges relevant information on cyberthreats and incidents occurring in Europe and informs the cooperation group of its activities, it is proposed that such information could also be shared with the EE-ISAC to ease effective communication that is specific to energy operators. Operators within the EE-ISAC are requesting to be an integral part of the NIS2 process of information exchange by national authorities, due to their responsibility for protecting infrastructure and energy services. Regarding Article 26 on the obligations to share between companies, operators expect to continue direct exchanges among TSOs and DSOs to manage energy sector responsibilities, preferring that the NCAs govern the process with their policy for sharing, rather than being an integral part of the actual information shared.

The EE-ISAC is looking to formalise their role within the new procedures and regulations. There are concerns that regulatory obligations to report incidents may leave the operators with less motivation to also share voluntarily within the ISAC, affecting engagement with ISAC platforms and opportunities. In a similar situation with energy audits, a qualitative difference was shown between voluntary and mandatory energy audits, with voluntary audits presenting a better quality with greater energy-saving improvements achieved than the mandatory audits [82]. Despite the onus on operators to share and report incidents under NIS arrangements, there is low confidence in receiving back useable threat information in a timely manner. Therefore, there is a strong desire to continue sharing between companies, especially if a 'tsunami' of data from incident reporting to authorities slows down information sharing that can be facilitated by national authorities.

The EE-ISAC will continue to be a combined voice for the energy sector to provide sector-specific feedback, anonymised where necessary, to the regulation and policy arena through its EU advocacy working group. The EE-ISAC aims to continue inviting the most appropriate stakeholders to the table to complement NIS2 and better support cross-border NCCS activities. The future role of the ISAC is also evolving towards being a connection into the private sector for the new Joint Cyber Unit [83].

7.8. Member Perception on ISAC Improving Cybersecurity Level of the Energy Sector (C08)

Membership of an ISAC needs to result in an improved cybersecurity level for member organisations and assist members to achieve their objectives under NIS2 and the NCCS, through developing best practices together and improving situation awareness. There will need to be a future assessment of members' perceptions and experiences of this to refine the ISAC platform and activities, ideally with performance measures in place to guide progress.

7.9. Trustworthiness

Another aspect that can be linked to applicability is the trustworthiness of a solution. This is particularly evident in relation to the artificial intelligence developments in recent years. Here, solid grounds for the assurance of the trustworthiness of a product or service are indispensable for its broader adoption [84,85]. Users seek confidence that the innovative solutions will act in a predictable manner that is favourable to their cause [86]. Additionally, Chaudhary et al. [87] consider trust next to usability and security in their broad survey of password managers. According to the study, the lack of trust poses a foremost problem, especially in relation to cloud-based or online systems. These questions are currently being reflected at the national and international strategic level [79,85].

Regarding the EE-ISAC, building trusting relationships amongst members of this newly formed network was crucial for optimal information sharing and collaboration. This was achieved through steady growth in member numbers and emphasising the requirement for member organisations to specify just one or two representatives to attend physical meetings without substitution to enable trust in the EE-ISAC space to grow among the same people attending meetings regularly. The representatives are required to sign confidentiality agreements. Close working relations have gradually been established, and seeing the same faces at EE-ISAC events was particularly effective at providing the consistency to build trust and a feeling of shared responsibility.

The predominant sharing activity in the EE-ISAC is between organisations that manage their energy and cyberinfrastructure. They interact in a network of trust, voluntarily sharing information to assist the energy sector as a whole. At this point, sharing between organisations is not automated, so most sharing and analysis actions within the ISAC currently involve a security practitioner. When member organisations begin to leverage the benefits of AI and ML within their operations, which could be exposed to adversaries, additional agreements between utility members to ensure appropriate protection and analysis ahead of sharing will ensure reliable information is being shared.

Awareness of the potential security downsides of holding a centralised information hub is prompting future work to improve the design of sharing mechanisms and increase the security, trust, and accuracy of information sharing. This will be further informed by the evolution of the NCCS, the outcomes of which will assist in defining use cases for sharing between operators in the synchronous grid area.

The EE-ISAC continues to work on providing actionable threat intelligence and tailoring the use of their sharing tools for the energy sector and EE-ISAC use cases. The process of creating the customisation of their platforms as a community is developing the trustworthiness of the shared tool. There have been deep-dive sessions held to develop the use cases and applicability of the platform to EE-ISAC needs. Threat intelligence and situational awareness is improved by defining their own structures and taxonomy for the data and contextualising the information. The use of nomenclature agreed by the community assists with labelling and querying the data for users to filter what they need. An indicator of trust can also be used to give insight on how much trust an analyst has in the information or the actor it is coming from.

8. Conclusions, Directions of Further Research, and Developments

The European Energy Information Sharing and Analysis Centre has been operating already for over six years. During this time, the platform has been joined by organisations from within and beyond the European Union. The members value the solution for being an instrument for enhancing cybersecurity cooperation beyond their individual organisations. The connections established among utility members have been supportive during challenging situations. The wider membership benefitted from the core group of utility members by gaining a better understanding of the needs and requirements of energy operators. The EE-ISAC network of trust forms a collaborative tool to mitigate risk. As a result, further membership applications are received, and yet a broader adoption of the solution is expected. The EU advocacy working group is positioning the EE-ISAC as the main reference organisation for cybersecurity in the European energy sector.

This situation is well-reflected in the results of the detailed analysis of applicability presented in this paper. Practically all areas from the control list have been completely addressed during the ISAC's development and operation. Regarding the continuity of support, the operation of the platform is accompanied by multiple events, including quarterly plenary meetings and training. The framework is continuously improved, based on the assessment results as well as in the context of the Empowering ISACs project. A potent community of EE-ISAC supporters has been established. The funding model is clearly described in the terms of reference. Similarly, the ISAC's documentation and supporting tools are provided to facilitate the use of the solution. The EE-ISAC's target-users are visibly indicated, among the other things, on the framework's website.

The effectiveness of the EE-ISAC was assessed by members during an interactive online plenary meeting. The study allowed for the identification of the improvement areas, which include reinforcing the ISAC's technical leadership and the analysis centre. Additionally, regular evaluations of the efficiency need to be carried out. These aspects and especially the operation of the analysis centre have a strong impact on the completeness of the results delivered by the association. Thus, further efforts to assure a more thorough contribution from the ISAC have been planned. Additionally, the complexity, usability, and acceptance properties of the EE-ISAC have been assisted with appropriate actions. To reduce the difficulties of understanding, describing, or (re)creating the EE-ISAC approach, the relevant topics were raised during meetings and events, and related documentation was published. For a higher precision of results and comprehensiveness of the ISAC's approach, further developments are envisaged, including the extension of situation awareness capability to consider both faults and attacks; the creation of more actionable threat intelligence; and engagement with interdependent sectors, such as the telecoms sector. As already mentioned, experts' subjective opinions regarding their impressions of using the solution were evaluated and provided important insights into further works. At the same time, the assessment of members' perceptions and experiences of the ISAC's improvements to the cybersecurity level of the energy sector still needs to be conducted.

The functional design of the EE-ISAC, with energy operators at the core of activities, ensures the continuity of relevant support, increasing the awareness and understanding of energy-specific cybersecurity. The utility of supporting tools will continue to be investigated during the current roll-out of the new information-sharing platform capability. Through the analysis of the EE-ISAC's approach with the applicability framework, recommendations have been made to improve the applicability and usefulness of this platform of cooperation for energy-sector participants. It contributes a road map for the ISAC to grow in maturity from the initial developments achieved so far to a more defined and managed role that also demonstrates the importance of the translation of cybersecurity to sectoral contexts. It also invites an opportunity to integrate EE-ISAC actions into the changing regulatory landscape and the cross-border cybersecurity requirements of the continental synchronous grid area. The main findings of the research are summarised in Table 4.

Table 4. Key achievements and future recommendations for the EE-ISAC.

Applicability Control Area	Key Achievements	Future Recommendations
Continuity of support (A01 to A04)	Value-added for members in cybersecurity cooperation across organisations. Improved understanding of energy sector context for cybersecurity practitioners. Regular events and training.	Leveraging collaborative approach requires innovation.
Documentation, tools, target-users, method evaluation, and completeness (B01 to B06)	Supportive documentation. Testing new research solutions in the energy context. Platform improvements, investigating utility of supporting tools.	Regular evaluations of efficiency. Develop analysis centre capability.
Complexity, usability, and acceptance properties (C01 to C08)	Energy operators at the core of activities have assisted useability and acceptance. Acts as a voice for the energy sector, provides feedback to policy arena.	Extension of situation awareness. Providing more actionable threat intelligence.

Author Contributions: Conceptualization, R.L.; methodology, R.L.; resources, T.W. and R.L.; writing—original draft preparation, T.W. and R.L.; writing—review and editing, T.W. and R.L.; visualization, T.W. and R.L.; funding acquisition, T.W. and R.L. All authors have read and agreed to the published version of the manuscript.

Funding: The support of this work through funding from the Engineering and Physical Sciences Research Council (EPSRC) grant number EP/L015471/1 and the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS) grant number EP/R022844/1 is gratefully acknowledged. RITICS have provided approval to publish this work.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Informed consent and approval to publish was obtained from EE-ISAC" in this context.

Data Availability Statement: Not applicable.

Acknowledgments: The support from EE-ISAC members during this work is gratefully acknowledged.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; or in the writing of the manuscript.

References

1. Leszczyna, R. Aiming at Methods' Wider Adoption: Applicability Determinants and Metrics. *Comput. Sci. Rev.* **2021**, *40*, 100387. [CrossRef]
2. Hong, J.B.; Kim, D.S.; Chung, C.-J.; Huang, D. A Survey on the Usability and Practical Applications of Graphical Security Models. *Comput. Sci. Rev.* **2017**, *26*, 1–16. [CrossRef]
3. Lantow, B.; Sandkuhl, K. An Analysis of Applicability Using Quality Metrics for Ontologies on Ontology Design Patterns. *Intell. Syst. Account. Financ. Manag.* **2015**, *22*, 81–99. [CrossRef]
4. Ling, L.W.; Downe, A.G.; Ahmad, W.F.W.; Lai, T.T. Determinants of Computer Usage among Educators: A Comparison between the UTAUT and TAM Models. In Proceedings of the 2011 National Postgraduate Conference, Seri Iskandar, Malaysia, 19–20 September 2011; pp. 1–6.
5. Deng, R.; Zhuang, P.; Liang, H. False Data Injection Attacks Against State Estimation in Power Distribution Systems. *IEEE Trans. Smart Grid* **2018**, *3053*, 1–10. [CrossRef]
6. Jhala, K.; Pradhan, P.; Natarajan, B. Perturbation-Based Diagnosis of False Data Injection Attack Using Distributed Energy Resources. *IEEE Trans. Smart Grid* **2021**, *12*, 1589–1601. [CrossRef]

7. Wang, Q.; Tai, W.; Tang, Y.; Zhu, H.; Zhang, M.; Zhou, D. Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. *Energies* **2019**, *12*, 2493. [CrossRef]
8. Leszczyna, R. *Cybersecurity in the Electricity Sector*; Springer: Cham, Switzerland, 2019; ISBN 978-3-030-19538-0.
9. Kotut, L.; Wahsheh, L.A. Survey of Cyber Security Challenges and Solutions in Smart Grids. In Proceedings of the 2016 Cybersecurity Symposium, Coeur d'Alene, ID, USA, 18–20 April 2016; pp. 32–37. [CrossRef]
10. Keshavarzi, M.; Ghaffary, H.R. I2CE3: A Dedicated and Separated Attack Chain for Ransomware Offenses as the Most Infamous Cyber Extortion. *Comput. Sci. Rev.* **2020**, *36*, 100233. [CrossRef]
11. Accenture. *Accenture 2021 Cyber Threat Intelligence Report*; Accenture: Chicago, IL, USA, 2021.
12. Sophos. *Sophos The State of Ransomware 2021*; Sophos: Abingdon, UK, 2021; ISBN 978-92-9204-536-4.
13. Liu, C.Z.; Zafar, H.; Au, Y.A. Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector. *Commun. Assoc. Inf. Syst.* **2014**, *34*, 15–36. [CrossRef]
14. Appan, R.; Bacic, D.; Madhavaram, S. Security Related Information Sharing among Firms: Potential Theoretical Explanations Completed Research. In Proceedings of the AMCIS 2018, New Orleans, LA, USA, 16–18 August 2018.
15. Appan, R.; Bacic, D. Impact of Information Technology (IT) Security Information Sharing among Competing IT Firms on Firm's Financial Performance: An Empirical Investigation. *Commun. Assoc. Inf. Syst.* **2016**, *39*, 214–241. [CrossRef]
16. Mermoud, A.; Keupp, M.M.; Huguenin, K.; Palmié, M.; David, D.P. To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing. *J. Cybersecur.* **2019**, *5*, 5. [CrossRef]
17. Leszczyna, R.; Wallis, T.; Wróbel, M.R. Developing Novel Solutions to Realise the European Energy—Information Sharing & Analysis Centre. *Decis. Support Syst.* **2019**, *122*, 113067. [CrossRef]
18. European Union Agency for Network and Information Security (ENISA). *Information Sharing and Analysis Center (ISACs)—Cooperative Models*; EU Publications: Luxembourg, 2018. [CrossRef]
19. Rashid, Z.; Noor, U.; Altmann, J. Economic Model for Evaluating the Value Creation through Information Sharing within the Cybersecurity Information Sharing Ecosystem. *Future Gener. Comput. Syst.* **2021**, *124*, 436–466. [CrossRef]
20. Yang, A.; Kwon, Y.J.; Lee, S.-Y.T. The Impact of Information Sharing Legislation on Cybersecurity Industry. *Ind. Manag. Data Syst.* **2020**, *120*, 1777–1794. [CrossRef]
21. Tosh, D.; Sengupta, S.; Kamhoua, C.A.; Kwiat, K.A. Establishing Evolutionary Game Models for Cyber Security Information EXchange (CYBEX). *J. Comput. Syst. Sci.* **2018**, *98*, 27–52. [CrossRef]
22. Gordon, L.A.; Loeb, M.P.; Lucyshyn, W. Sharing Information on Computer Systems Security: An Economic Analysis. *J. Account. Public Policy* **2003**, *22*, 461–485. [CrossRef]
23. Gal-Or, E.; Chose, A. The Economic Incentives for Sharing Security Information. *Inf. Syst. Res.* **2005**, *16*, 186–208. [CrossRef]
24. Hausken, K. Information Sharing among Firms and Cyber Attacks. *J. Account. Public Policy* **2007**, *26*, 639–688. [CrossRef]
25. Liu, D.; Ji, Y.; Mookerjee, V. Knowledge Sharing and Investment Decisions in Information Security. *Decis. Support Syst.* **2011**, *52*, 95–107. [CrossRef]
26. Vakilinia, I.; Sengupta, S. A Coalitional Game Theory Approach for Cybersecurity Information Sharing. In Proceedings of the 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017; pp. 237–242.
27. Tosh, D.; Sengupta, S.; Kamhoua, C.; Kwiat, K.; Martin, A. An Evolutionary Game-Theoretic Framework for Cyber-Threat Information Sharing. In Proceedings of the IEEE International Conference on Communications, London, UK, 8–12 June 2015; pp. 7341–7346.
28. Ghose, A.; Hausken, K. A Strategic Analysis of Information Sharing Among Cyber Attackers. *J. Inf. Syst. Technol. Manag.* **2015**, *12*, 245–270. [CrossRef]
29. Nikoofal, M.E.; Zhuang, J. On the Value of Exposure and Secrecy of Defense System: First-Mover Advantage vs. Robustness. *Eur. J. Oper. Res.* **2015**, *246*, 320–330. [CrossRef]
30. Zhuang, J.; Bier, V.M.; Alagoz, O. Modeling Secrecy and Deception in a Multiple-Period Attacker-Defender Signaling Game. *Eur. J. Oper. Res.* **2010**, *203*, 409–418. [CrossRef]
31. Zhuang, J.; Bier, V.M. Reasons for Secrecy and Deception in Homeland-Security Resource Allocation. *Risk Anal.* **2010**, *30*, 1737–1743. [CrossRef] [PubMed]
32. Sedenberg, E.M.; Mulligan, D.K. Public Health as a Model for Cybersecurity Information Sharing. *Berkeley Technol. Law J.* **2015**, *30*, 1687. [CrossRef]
33. Bourgue, R.; Budd, J.; Homola, J.; Wlasenko, M.; Kulawik, D. *Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs*; EU Publications: Luxembourg, 2013.
34. de Fuentes, J.M.; González-Manzano, L.; Tapiador, J.; Peris-Lopez, P. PRACIS: Privacy-Preserving and Aggregable Cybersecurity Information Sharing. *Comput. Secur.* **2017**, *69*, 127–141. [CrossRef]
35. van Impe, K. How STIX, TAXII and CybOX Can Help with Standardizing Threat Information. Available online: https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/ (accessed on 24 April 2019).
36. Fransen, F.; Smulders, A.; Kerkdijk, R. Cyber Security Information Exchange to Gain Insight into the Effects of Cyber Threats and Incidents. *e i Elektrotechnik Inf.* **2015**, *132*, 106–112. [CrossRef]
37. Qamar, S.; Anwar, Z.; Rahman, M.A.; Al-Shaer, E.; Chu, B.T. Data-Driven Analytics for Cyber-Threat Intelligence and Information Sharing. *Comput. Secur.* **2017**, *67*, 35–58. [CrossRef]

38. Vakilinia, I.; Tosh, D.K.; Sengupta, S. Privacy-Preserving Cybersecurity Information Exchange Mechanism. In Proceedings of the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Seattle, WA, USA, 9–12 July 2017; pp. 1–7.
39. Jajodia, S.; Noel, S.; Kalapa, P.; Albanese, M.; Williams, J. Cauldron: Mission-Centric Cyber Situational Awareness with Defense in Depth. In Proceedings of the IEEE Military Communications Conference MILCOM, Baltimore, MD, USA, 7–10 November 2011; pp. 1339–1344.
40. Locasto, M.E.; Parekh, J.J.; Keromytis, A.D.; Stolfo, S.J. Towards Collaborative Security and P2P Intrusion Detection. In Proceedings of the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, West Point, NY, USA, 15–17 June 2005; Volume 2005, pp. 333–339.
41. Zhang, T.; Zhu, Q. Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs. *IEEE Trans. Signal Inf. Process. Over Netw.* **2018**, *4*, 148–161. [CrossRef]
42. Patel, A.; Alhussian, H.; Pedersen, J.M.; Bounabat, B.; Júnior, J.C.; Katsikas, S. A Nifty Collaborative Intrusion Detection and Prevention Architecture for Smart Grid Ecosystems. *Comput. Secur.* **2017**, *64*, 92–109. [CrossRef]
43. Abdellatif, T.; Mosbah, M. Efficient Monitoring for Intrusion Detection in Wireless Sensor Networks. *Concurr. Comput. Pract. Exp.* **2017**, *32*, e4907. [CrossRef]
44. Liu, X.; Zhu, P.; Zhang, Y.; Chen, K. A Collaborative Intrusion Detection Mechanism against False Data Injection Attack in Advanced Metering Infrastructure. *IEEE Trans. Smart Grid* **2015**, *6*, 2435–2443. [CrossRef]
45. ECOSSIAN. European Control System Security Incident Analysis Network (ECOSSIAN) Project Website. Available online: http://ecossian.eu/ (accessed on 11 December 2018).
46. Kaufmann, H.; Hutter, R.; Skopik, F.; Mantere, M. A Structural Design for a Pan-European Early Warning System for Critical Infrastructures. *e i Elektrotechnik Inf.* **2015**, *132*, 117–121. [CrossRef]
47. Barth, R.; Meyer-Nieberg, S.; Pickl, S.; Schuler, M.; Wellbrink, J. A Toolbox for Operational Analysis. In *Emerging and Applications of M & S in Industry and Academia Symposium, Proceedings of the EAIA 2012, Orlando, Florida, USA, 26–30 March 2012*; Society for Computer Simulation International: San Diego, CA, USA, 2012; pp. 106–113.
48. Klump, R.; Kwiatkowski, M. Distributed IP Watchlist Generation for Intrusion Detection in the Electrical Smart Grid. *IFIP Adv. Inf. Commun. Technol.* **2010**, *342*, 113–126. [CrossRef]
49. Brunner, M.; Hofinger, H.; Roblee, C.; Schoo, P.; Todt, S. Anonymity and Privacy in Distributed Early Warning Systems. In Proceedings of the Critical Information Infrastructures Security; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6712, pp. 81–92.
50. Alcaraz, C.; Lopez, J. Wide-Area Situational Awareness for Critical Infrastructure Protection. *Computer* **2013**, *46*, 30–37. [CrossRef]
51. Marchetti, M.; Pierazzi, F.; Colajanni, M.; Guido, A. Analysis of High Volumes of Network Traffic for Advanced Persistent Threat Detection. *Comput. Netw.* **2016**, *109*, 127–141. [CrossRef]
52. Friedberg, I.; Skopik, F.; Settanni, G.; Fiedler, R. Combating Advanced Persistent Threats: From Network Event Correlation to Incident Detection. *Comput. Secur.* **2015**, *48*, 35–57. [CrossRef]
53. Coppolino, L.; D'Antonio, S.; Formicola, V.; Romano, L. A Framework for Mastering Heterogeneity in Multi-Layer Security Information and Event Correlation. *J. Syst. Archit.* **2016**, *62*, 78–88. [CrossRef]
54. Pala, A.; Zhuang, J. Information Sharing in Cybersecurity: A Review. *Decis. Anal.* **2019**, *16*, 172–196. [CrossRef]
55. He, M.; Devine, L.; Zhuang, J. Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk Anal.* **2018**, *38*, 215–225. [CrossRef] [PubMed]
56. High Representative of the EU for Foreign Affairs and Security Policy. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*; High Representative of the EU for Foreign Affairs and Security Policy: Brussels, Belgium, 2013.
57. Baldwin, R.; Cave, M.; Lodge, M. *Understanding Regulation: Theory, Strategy and Practice*; Oxford University Press: Oxford, UK, 2012; ISBN 978-0-19-957609-8.
58. Swarz, R.S.; de Rosa, J.K. *A Framework for Enterprise Systems Engineering Processes*; The MITRE Corporation: Bedford, MA, USA, 2006.
59. Christensen, K.K.; Petersen, K.L. Public-Private Partnerships on Cyber Security: A Practice of Loyalty. *Int. Aff.* **2017**, *93*, 1435–1452. [CrossRef]
60. Leszczyna, R. Review of Cybersecurity Assessment Methods: Applicability Perspective. *Comput. Secur.* **2021**, *108*, 102376. [CrossRef]
61. Leszczyna, R. Practical Cybersecurity Assessment Techniques—Why Are They Adopted? A Review, Determinants and the Applicability Checklist. *Comput. Sci. Rev.* 2022, *submitted*.
62. Juriado, R.; Gustafsson, N. Emergent Communities of Practice in Temporary Inter-Organisational Partnerships. *Learn. Organ.* **2007**, *14*, 50–61. [CrossRef]
63. Trim, P.R.J.; Lee, Y.-I. The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement. *Big Data Cogn. Comput.* **2021**, *5*, 32. [CrossRef]
64. Innovation and Networks Executive Agency. *2020 CEF Telecom Call-Cybersecurity (CEF-TC-2020-2)*; Innovation and Networks Executive Agency: Brussels, Belgium, 2020.

65. Smith, P.; Wallis, T.; Skouloudi, C.; Moulinos, K.; Harsch, A.; Staggenborg, M.; Rocca, M.; dos Santos, D.; Bouhdada, J.; Kulicke, M.; et al. Cyber Security Incident Response. 2020. Available online: https://www.ee-isac.eu/comp/uploads/2020/12/EE-ISAC-Incident-Response-White-Paper-1.pdf (accessed on 15 February 2022).
66. Rocca, M.; Schauer, S.; Smith, P.; Wolthuis, R. Cyber Security Risk Management for Digitalized Energy Systems: Challenges & Solutions. 2018. Available online: https://www.ee-isac.eu/wp-content/uploads/2020/01/EE-ISAC-White-Paper-Risk-Management.pdf (accessed on 15 February 2022).
67. Harsch, A.; Kulicke, M.; Moulinos, K.; Seiler, A.; Skouloudi, C.; Zisi, A. *Threat Intelligence Management*; EE-ISAC: Brussels, Belgium, 2020; Available online: https://mcusercontent.com/fac8062360203f4bc7e2b068e/files/43469184-8757-477c-8780-d899293cbac0/Threat_Management_Master_v1.2_ENISA_Proofreading_SA.01.pdf (accessed on 15 February 2022).
68. ENISA. *ENISA Threat Landscape*; ENISA: Athens, Greece, 2021.
69. Vmoso. Vmoso Case Study: EE-ISAC Thwarting Cyber Threats to European Energy Infrastructure through Collaboration. Available online: https://vmoso.com/vmoso/ee-isac-thwarting-cyber-threats-to-european-energy-infrastructure-through-collaboration/ (accessed on 7 February 2022).
70. Bochman, A.A.; Freeman, S. *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)*; CRC Press: Boca Raton, FL, USA, 2021.
71. Empowering Information Analysis Centres. Available online: https://www.isacs.eu/ (accessed on 4 February 2022).
72. European Union Agency for the Cooperation of Energy Regulators. *Framework Guideline on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows*; European Union Agency for the Cooperation of Energy Regulators: Ljubljana, Slovenia, 2021.
73. ENTSO-E & E.DSO. *Recommendations for the European Commission on a Network Code on Cybersecurity*; ENTSO-E & E.DSO: Brussels, Belgium, 2021.
74. EE-ISAC. *Consultation Questionnaire on the Draft Framework Guideline on Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows*; EE-ISAC: Brussels, Belgium, 2021.
75. Liu, R.; Vellaithurai, C.; Biswas, S.S.; Gamage, T.T.; Srivastava, A.K. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Trans. Smart Grid* **2015**, *6*, 2444–2453. [CrossRef]
76. Ganjkhani, M.; Gilanifar, M.; Giraldo, J.; Parvania, M. Integrated Cyber and Physical Anomaly Location and Classification in Power Distribution Systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7040–7049. [CrossRef]
77. Burns, M.G. Participatory Operational & Security Assessment on Homeland Security Risks: An Empirical Research Method for Improving Security beyond the Borders through Public/Private Partnerships. *J. Transp. Secur.* **2018**, *11*, 85–100. [CrossRef]
78. 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*; European Commission: Brussels, Belgium, 2020.
79. Department of Homeland Security. *S&T Artificial Intelligence and Machine Learning Strategic Plan*; Department of Homeland Security: Washington, DC, USA, 2021.
80. Mee, P.; Chandrasekhar, C. *Cybersecurity Is Too Big a Job for Governments or Business to Handle Alone*; European Union Agency for Law Enforcement Training (CEPOL): Budapest, Hungary, 2021.
81. EE-ISAC. *EE-ISAC Position on Proposal for a Directive on the Resilience of Critical Entities*; EE-ISAC: Brussels, Belgium, 2021.
82. Krutwig, M.C.; Tanțău, A. Obligatory versus Voluntary Energy Audits: Are There Differences in Quality? *Proc. Int. Conf. Bus. Excell.* **2018**, *12*, 522–532. [CrossRef]
83. European Commission Factsheet: Joint Cyber Unit. Available online: https://digital-strategy.ec.europa.eu/en/library/factsheet-joint-cyber-unit (accessed on 4 February 2022).
84. Apruzzese, G.; Andreolini, M.; Ferretti, L.; Marchetti, M.; Colajanni, M. Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems. *ACM J.* **2021**. [CrossRef]
85. European Commission. *Whitepaper on Artificial Intelligence—A European Approach to Excellence and Trust*; European Commission: Brussels, Belgium, 2020.
86. Blatt, N. Operational Trust: A New Look at the Human Requirement in Network Centric Warfare; 9th International Command and Control Research and Technology Symposium Coalition Transformation: An Evolution of People, Processes, and Technology to Enhance Interoperability. 2004. Available online: https://apps.dtic.mil/sti/pdfs/ADA466612.pdf (accessed on 15 February 2022).
87. Chaudhary, S.; Schafeitel-Tähtinen, T.; Helenius, M.; Berki, E. Usability, Security and Trust in Password Managers: A Quest for User-Centric Properties and Features. *Comput. Sci. Rev.* **2019**, *33*, 69–90. [CrossRef]