
# How can we design a socio-technical, interorganisational response to ensure better cybersecurity for Critical Infrastructure?

PhD Thesis

Tania Wallis

Department of Electronic & Electrical Engineering

University of Strathclyde, Glasgow

8 March 2023

# Abstract

The monitoring and control of critical infrastructures enables greater efficiencies and more effective operation. However, growing complexities across these interconnected systems brings a higher risk of cyber-attack. This thesis explores the organisational and regulatory aspects of improving the cybersecurity of Critical Infrastructure, proposing a cooperative socio-technical response across public and private actors. Alongside a transforming energy sector, to integrate renewable generation and electrify heat and transport, a significant cybersecurity response is also required. This research provides a thorough investigation of cybersecurity concerns of energy utilities to explain their organisational and sectoral context.

A case study of public-private partnership in the European energy sector serves to demonstrate private actors fostering public values to protect grid networks and energy services. This evidence-based analysis of the formation of an ISAC demonstrates the qualities that built a trusted network and deepened cooperation among energy sector participants both within Europe and globally. It recommends a new approach going forward for the ISAC to integrate their actions into the changing regulatory landscape and cross-border requirements of the continental synchronous grid area.

A study of interorganisational cooperation within the context of securing supply chains to critical infrastructure contributes a cross-industry comparison of the UK's implementation of the NIS Directive. This compares experiences in Energy, Water & Aviation evaluating their response to NIS interventions and the extent of their ability to oversee supply chain cybersecurity. It recommends an approach to supply chain oversight to achieve a balance between control and cooperation, that enhances the existing UK NCSC guidance. These insights can be more broadly applied now that NIS2 proposes all member states include supply chain responsibilities in their NIS expectations.

Central to this work was the need to establish an orient function, as a foundation for energy operators to orient themselves among the interdependencies of critical infrastructure, to better understand their place and responsibility to secure assets and services, for their own business and for the energy system as a whole. The multi-actor collaborative approach proposed, and validated in practice groups, establishes a necessary Orientation function and enables a clearer understanding of cybersecurity risk by all participants.

# Contents

# List of Figures

# List of Tables

# Acknowledgments

I wish to express my immense gratitude for all the support and guidance I have received from many kind people during this PhD journey. I am hugely grateful for all the patience and encouragement of my supervisor Dr James Irvine, for all my colleagues and supporters at Strathclyde, PNDC, Glasgow and EE-ISAC, for industry sponsors at Frazer Nash and Rolls Royce for helping me find my way, for the moral support of friends and colleagues continuing to believe in me throughout. And most of all, I am forever grateful to my family for accommodating my PhD journey amongst some extremely difficult years for us all.

# Publications

Some content from this thesis has already been published in the following publications:

1. Tania Wallis, Greig Paul, and James Irvine, “Organisational Contexts of Energy Cybersecurity,” Conference Proceedings SPOSE2021 at ESORICS. Lecture Notes in Computer Science, vol 13106. Springer. doi.org/10.1007/978-3-030-95484-0_22
2. Tania Wallis, and Rafał Leszczyna. 2022. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector" Energies 15, no. 6: 2170. doi.org/10.3390/en15062170
3. Tania Wallis, and Chris Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-10, doi: 10.1109/CyberSA49311.2020.9139641
4. Tania Wallis, Chris Johnson, and Mohamed Khamis. "Interorganizational cooperation in supply chain cybersecurity: a cross-industry study of the effectiveness of the UK implementation of the NIS Directive." Information and Security: An International Journal 48, no. 1 (2021): 36-68. https://doi.org/10.11610/isij.4812
5. Tania Wallis, and Paul Dorey, “Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience”. Energies 2146564 (ISSN 1996-1073), Section C: Energy Economics and Policy, Special Issue on Energy Communities Implementation 2022. https://doi.org/10.3390/en16041868
6. Tania Wallis. Achieving cybersecurity improvements through Enterprise Systems Engineering. ASEC 2020 Conference, 17-18 Nov 2020. eprints.gla.ac.uk/228994/
7. Rafał Leszczyna, Tania Wallis, Michał R. Wróbel, “Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre”. Decision Support Systems, Volume 122, 2019. https://doi.org/10.1016/j.dss.2019.05.007
8. Tania Wallis, Richard James Thomas, John Dickinson, and Chris Johnson, “Resolving anti-patterns in ICS”. 2021. Industry guidance reviewed by UK NCSC technical authors and in use by NCSC ICS-COI, will shortly be published on ICS-COI web presence to be hosted under RITICS.org.

# 1 Introduction

This chapter introduces the research problem and outlines the key aims of this research.

## 1.1 Holistic Engineering

Energy distribution is becoming increasing complex and involving many more actors. This presents many challenges to providing effective security of energy services, especially since the problem spans both technical and organisational aspects. As such, the energy sector is a good example of where a more holistic approach to engineering may yield better results. The author came to this work with an interest in holistic engineering, as a practice that considers the broader dimensions in each design challenge, looking at many aspects of a problem including the impact and consequences of innovation. This approach requires communication across disciplines and is enabled by experiential spaces that bring together different skillsets and exercise the ability to bridge skill areas [1].

## 1.2 What is 'special' about the energy sector

The backdrop to the culture of interaction in the energy sector is the electricity grid itself. Its wholly interconnected nature makes it technically paramount that a continuous real-time balancing of the AC system meets the energy supply and demand needs of all that is interconnected to it. Furthermore, introducing internet connected devices for monitoring and control of the system adds another layer of interconnectivity. Operating with both the electricity synchronous grid connection, and internet connectivity in the control layer, exacerbates the interdependencies. The grid system has protection mechanisms working within network constraints, making it particularly sensitive to the risk of cascading effects that have the potential to result in cascading power outages. This built-in sensitivity is an essential and critical safety mechanism for a system utilising high line voltages and for effective system balancing of electricity supply and demand.

Having this technical design in mind influences the culture of organisations managing the energy networks. The understanding of impact and consequences to the electricity grid, and the duty to keep the lights on, encourages closer interworking between organisations.

## 1.3 Digitalisation of energy systems

The increasing use of automation and expansion of monitoring and control capability across the power system and other critical infrastructures is enabling greater efficiencies and more

effective operation [2] [3]. However, the growing complexity across these interconnected systems also exposes the system to a higher risk of cyber-attack, including the potential to cause physical damage [4]. Emerging power network concepts and advances in information and communication technologies, consumer and demand side technologies, and the integrated systems required to deliver future energy services, potentially expose the grid system to a new and significant level of cybersecurity threat [5] [6].

The digitalisation of energy is enabling improved visibility of energy systems and facilitating a larger share of distributed renewable generation. Monitoring and controlling energy infrastructure involves the use of Supervisory Control & Data Acquisition (SCADA), Active Network Management capability, machine learning for predictive maintenance and more. Balancing supply and demand of electricity relies on data analytics for forecasting, and the management of flexibility services across multiple providers.

The integration effort at a technical level to optimise management of energy systems also requires layers of security to be deployed, such as segmentation of networks based on how the technology will be used and by whom, considering both authorized and malicious actors. If an IT or OT network becomes compromised, it is important to prevent lateral movement by an attacker across the network to find and impact more critical assets.

The fast-changing nature of technology is expecting knowledge and skillsets to evolve. Previous 'experts' are having to adapt to a new and changing system. This work supports such an evolution of knowledge by bringing together different skillsets into practice groups.

## 1.4 Cybersecurity context

The evolution of a 'smarter' grid brings an increasingly distributed environment, a wider spread of intelligent and connected devices, and an expansion of the potential attack surface to malicious actors. In particular, embedded devices controlling the safe operation of physical equipment are most critical and also most vulnerable. However, many embedded devices in the power system do not currently support encryption or authentication or antivirus. Until security features can be added or devices replaced they depend on secure architectures to restrict access. Such architectures will themselves have vulnerabilities making protection from malicious acts an ongoing challenge. The increasing use of communications for access to devices and control systems is growing the need to provide secure networks, secure communications across those networks and secure access to management systems, see Figure 1.

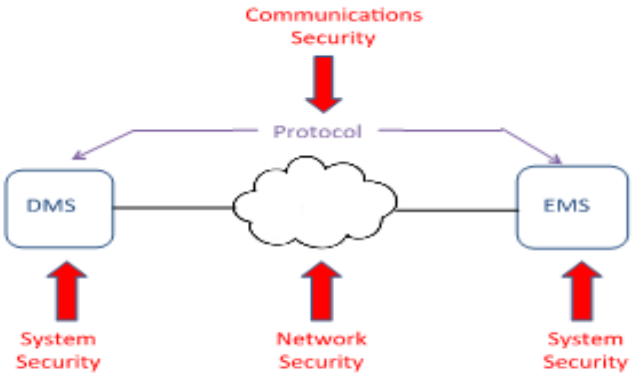


*Figure 1 Perspectives on cyber security*

Approaches to cyber security developed in the IT world do not easily apply to the needs of an ICS, especially due to availability being a top priority to ensure uninterrupted continuity of supply, see Figure 2. Enterprise security focuses on protecting data in servers. ICS security aims to protect the ability to operate safely and securely. For example, in the power system, providing continuous power flow is seen as more important than ensuring information about power flows is confidential.


Figure 2 Availability as top priority

To achieve a balance of Availability, Integrity and Confidentiality (AIC), Table 1 sets out some requirements that would contribute to ensuring AIC.

| | Requirements to achieve AIC |
|---|---|
| A Availability | Preventing disruption of service and productivity.<br>Ensuring resources are accessible when needed by an authorised party. |
| I Integrity | Ensuring desired resource contains accurate information and performs as intended.<br>Preventing unauthorised modification of systems and information.<br>Linking actions to actors – non-repudiation – to prevent an actor from denying an action. |
| C Confidentiality | Making sure resources are only accessible to the desired person or system.<br>Preventing unauthorised disclosure of systems or information.<br>Checking identity through authentication and authorisation. |

Table 1 Achieving Availability-Integrity-Confidentiality

Organisations cannot go it alone to manage their cybersecurity effectively – there is a necessity to work together. Furthermore, the integration of power networks, energy systems, digital control, communications networks, information and operational technologies, makes up a complex space from which to secure energy services. During this research, industry partners were often asking "What do we need to do?" and "How much is enough?" The contribution of this research intends to provide assistance with navigating this complexity.

## 1.5 Aims of the research

**Research Question: How can we design a socio-technical, interorganisational response to ensure better cybersecurity for Critical Infrastructure?**

Within this research question, the key aims of this research are as follows:

- To develop a framework to enable interorganisational responses to cybersecurity relevant to the Operational Technology (OT) context.
- To establish an orient function, building capability to adapt and reposition through better understanding of the OT context for both technical and policy implementations.
- To provide an exemplar of integrating knowledge spaces to bring cybersecurity to the energy context.

## 1.6 Industry support for this work

The research challenge area for this PhD was proposed by industry sponsor Frazer-Nash Consultancy and supported by Rolls-Royce and Scottish and Southern Energy. It centres around securing Industrial Control System (ICS) installations to an appropriate level by considering how much cybersecurity is 'enough' and what organisations need to do to be secure. The intention was to provide organisations with a pragmatic approach to identifying and meeting their ICS cybersecurity assurance requirements and to help organisations determine how to approach cybersecurity as the 'elephant in the room' of rapid digitalisation and transformation of the energy sector. The increasingly distributed nature of the future power system presents operational impacts that can go beyond organisational structures such that cybersecurity responsibilities become blurred.

# 2 Methodology

This chapter describes the methods utilised at each stage of this research, and places the thesis within the context of related works.

Due to the necessity for organisations to work together to manage their cybersecurity more effectively, this research set out to exercise interorganisational responses, aiming to build adaptability to the increasing need for cybersecurity improvements, through interworking between organisations. This involved setting up practice spaces, and identifying opportunities for working together, as well as researching progress within organisations and their contributions to cybersecurity from individual companies.

This research utilises an interdisciplinary approach by transferring knowledge between areas to define new knowledge and practices that are specifically for digitalised Operational Technology environments. It also includes transdisciplinary characteristics by focussing on real-world problems and involving non-academic participants in the process, and by working with a transformative approach to proactively support actions and interventions, and through continually reflecting on the broader contexts by providing impact beyond academic outputs [7]. The research has an applied orientation to contribute towards improving practices.

## 2.1 Practice spaces

The utilisation of practice spaces, as a common thread of activity throughout this thesis, has brought together different perspectives and expertise to create a synthesis of knowledge that is solution-oriented towards the cybersecurity needs of a digitalising energy sector. It required both academic and non-academic actors to engage in a process of co-creating new knowledge.

The foundation for each practice space was to convene a group of potential collaborators with a shared interest in energy cybersecurity. In each case a review of the skillsets, knowledge and experience of the members present built an understanding of the expertise in the groups. Introducing the problem area set the common ground for the collaboration, for each participant to strive towards. Developing and communicating a shared vision, the group would proceed with an integrative approach to combine skillsets through a process of sharing and analysis, to form a synthesis of experiences and practices. Where possible this

was then translated into actionable guidance to enable cybersecurity improvements suitable for an OT context. The author's role predominantly involved being between disciplines rather than in any one area of expertise to guide the coming together. The activities of these practice spaces can be summarised as follows:

- Define the reason for the practice space, introducing the challenge and the problem to be addressed.
- Convene the group – inviting different perspectives on the issue to enrich the work with multiple perspectives.
- Set the common ground for the collaboration – with rules of engagement.
- Develop and communicate a shared vision together, defining the context for the practice.
- Know the group – meet them where they are – get to know the knowledge, experience, and expertise in the group. To meet them where they're at and invite contributions, with the goal in mind and the objective communicated.
- The Synthesis – A process of sharing and analysis, to form a synthesis of experiences and practices. Broadening perspectives. Addressing gaps. Together constructing new knowledge.
- Creative effort, co-producing outputs – Content provided from different experts is reviewed by all and discussed in meetings to develop further insights together. Translation of the work into actionable guidance to enable cybersecurity improvements suitable for an OT context to be shared beyond the practice group.

The above actions are not necessarily sequential, some may happen alongside another or be revisited. These are common activities that have been used as a framework to guide each unique practice group. This approach has since been applied in future work to form the Supply Chain Cybersecurity expert group for OT which involves several different sectors.

## 2.2 Orienting

In addition to co-creating guidance and improvements, the journey towards such outcomes was in each case an exercise in adapting and repositioning to embed cybersecurity into an OT context. In comparing Industrial Control System (ICS) design with defence tactics, military operations aim to execute the OODA loop (Observe Orient Decide Act) faster than an adversary [8]. Automated control systems tend to:

- Observe with sensors
- Decide with a comparator
- Take action via actuators

They typically have no Orient function.

There is a need for operators to orient themselves amongst the interdependencies of critical infrastructure and to better understand their place and responsibility in securing these assets and the services they provide to society. A resilient system needs to orient itself, to notice and discover when in an unexpected or new situation, then recover itself into an acceptable operating band with cooperation and collaboration of peers [9]. Enabling both a system and procedural response to events, combining secure technology with secure organisational capability, can build a stronger framework for resilience.

The need to exercise the process of Orienting is particularly relevant to the fast-changing environment of digitalisation. OT with its safety knowledge has previously operated as a separate entity to IT. The previously used mental models of either IT or OT, applied in isolation, no longer works for a changing environment that integrates both and requires a new approach to manage. The process of orienting is to continually adjust to a new picture of things, to be able to deconstruct what worked before and reconstruct for a new situation. IT and OT and safety expertise are needing to consider the many factors influencing their operation and apply new models in an interconnected way to arrive at methods suitable for an evolving sector, approaches that fit the new reality.

The approach of interorganisational cooperation and partnership explored in this thesis offer a means to establishing this orient function and are an essential foundation of cybersecurity governance. The practice spaces conducted during this research were all exercising the process of orienting practitioners to the OT context and a digital energy sector.

Table 2 shows different areas of activity that can be distinguished, from solving one-off problems to looking at longer term capability, using an exploratory mindset or achieving closure with decisions and actions. All four activities play a role in effective preparations.
“Systems cannot be constructed to eliminate security risk” [10] so it is essential that systems are designed to recognise, resist and recover from attacks. Longer term considerations and

the ability to adapt to new threats are important for systems to sustain assurance over time. A continued adaptation is necessary to respond both to changes in threats and changes in functions or usage of the system that could enable an attack.

| | Single Activity<br>**Problem Solving** | Ongoing Activity<br>**Surviving/thriving** |
|---|---|---|
| Opening Up<br>**Exploration** | What's going on?<br>Making sense of the latest threat landscape. | What's coming?<br>Anticipation<br>Preparedness |
| **Closure**<br>Decisions | Developing a Strategy<br>to deal with cybersecurity. | Organisational Learning<br>Adapting to changes and new threats.<br>Dynamic response. |

Table 2 Dimensions of purposeful activity [11]

This research initially focussed on the opening up and exploratory dimension of Table 2 to provide an improved awareness and understanding of the situation and context of future energy networks. Latter stages included action research involving stakeholders in organisational learning and improvements towards meeting strategic objectives in cybersecurity.

## 2.3 Participant Observation

The author was able to experience the Operational Technology theme in a variety of settings as a participant observer. This included involvement in the network of academic and industry members of PNDC, taking an active role in the start-up stage of an ISAC supporting the Board of EE-ISAC, and by forming a Supply Chain Expert Group for the UK NCSC. These participant observer opportunities were a significant aid to understanding the environment in which CI cybersecurity practitioners work. The author was able to be closer to the problem area and to include the experiences of those immersed in an OT context, and arrive at more effective and relevant outcomes [12].

### 2.3.1 Participation in the ISAC

The author became an academic member of the European Energy Information Sharing and Analysis Centre (ISAC) and held the role of Secretariat for the ISAC for 3 years. The EE-ISAC provided an opportunity to step into a 'third' space away from the more remote position of academia, to be involved in the energy OT community as a participant observer at the centre of a newly forming ISAC. Taking on an active role, constructed by the ISAC setting, with

Secretariat responsibilities, immersed the author very much at the centre of the community and all its subgroups. During research activities, some level of participation is important to build and sustain trusted relations and there was also a duty of reciprocity for entering into the ISAC with expectations on members to provide in-kind contributions. The author's role essentially involved coordinating the start-up years of the ISAC, implementing the prototype of a first cross-border ISAC for the energy sector, while fostering cooperative partnerships in cybersecurity. The experience and practice of creating this ISAC informed the content of 'ISAC-in-a-box' [13] by ENISA to support and encourage newer ISACs. The EE-ISAC is now used as an example ISAC for other sectors and their learning and experience is often used to inform the formation and development of newer ISACs.

Figure 3 shows the coverage of EE-ISAC by members' countries shown in red.

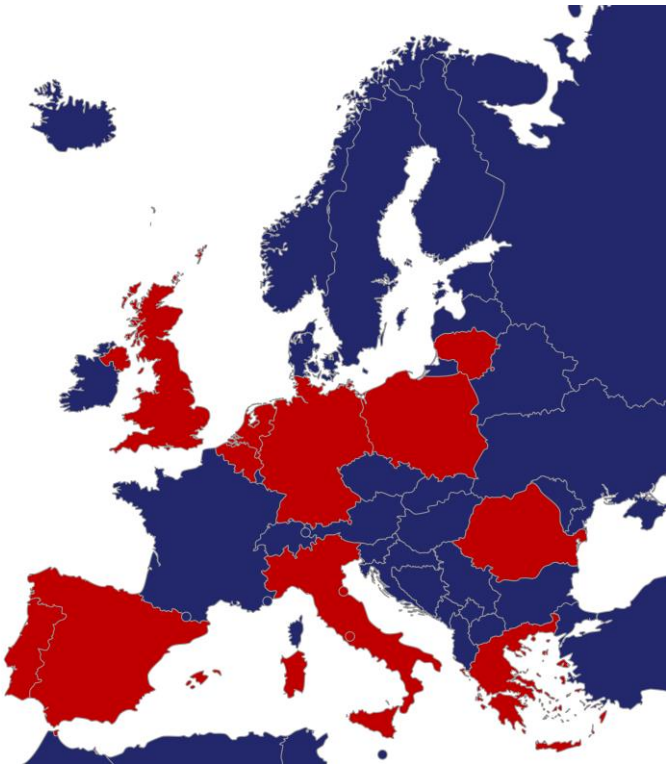

*Figure 3 EE-ISAC member countries*

Once the membership contributions were sufficient to fund both the Marketing and Secretariat services from a strategic consulting group in Brussels, the author was able to commence a gradual exit from the role while upskilling personnel to take on Secretariat responsibilities. The author remained engaged as an academic member and being at the

centre of defining ISAC activities enabled an academic contribution to be developed alongside practical progress.

## 2.4 Defining the Energy Cybersecurity Context

The first stage of this research was carried out within the academia and industry network of the Power Network Demonstration Centre (PNDC) at University of Strathclyde. This was during the evolution of a new research theme at the PNDC to include Communications and Systems Integration alongside the already established Power Networks research themes. This was bringing together Power Systems experts with Communications engineers, and cybersecurity was also being introduced as a new topic that needed to be integrated into existing knowledge areas, alongside the launch of this new Communications and Systems Integration research theme. The PNDC themes, alongside whole energy systems research, are supporting the evolution of Distribution Network Operators (DNOs) into Distribution System Operators (DSOs) to take on additional responsibilities for balancing supply and demand on distributed renewable energy networks.

This first practice space included 20 people with cybersecurity responsibilities in UK based operations from a spread of organisations including five energy companies, three telecom service providers, two suppliers of automation & smart grid equipment, two consultancies. The different skillsets being combined included IT security, OT engineers, and Telecoms experts. This stage aimed to define the context of OT cybersecurity, integrating the required knowledge spaces, bringing together the interorganisational participants, with the goal of achieving a synthesis of skillsets and knowledge that the context of OT cybersecurity required. This created the foundations of a practice space that also enabled further work by the group.

Key concerns and issues for Distribution Network Operators (DNOs) on achieving cybersecurity of future energy scenarios were evaluated through their participation in semi-structured interviews and in workshop group discussions. This enabled a backdrop of shared understanding for the ongoing development of cybersecurity implementations in the sector to be formed. Several round-table discussions, with different skillsets in each invited an open exploration of the issues to form the organisational context of a future Distribution System Operator (DSO).

### 2.4.1 Workshop process

Cybersecurity approaches and mitigations must consider the wider engineering solution and the operational and cultural context they need to function within. The aim of the workshop was *to* provide an improved awareness and understanding of the cybersecurity situation of future energy networks and together define the context to improve preparedness and applicability of actions to an OT environment. To share the knowledge and experience of the group, there were presentations given from cybersecurity and risk management experts and to set the scene a presentation on cyber threats in operational networks.

The workshop attendees were split into three groups. Group membership was determined beforehand, with a coloured sticker on the name badges, to ensure a diversity of experience in each group. The group facilitator was responsible for keeping time and tracking the answering of questions and taking notes. All groups had the same question set. In addition to the questions listed in Table 3, the opportunity to brainstorm thoughts onto post it notes was also given, as well as some free discussion in groups to make the most of the skills and experiences present, and to encourage contribution from all parties.

| | **Workshop & Interview Question Set** |
|---|---|
| 1 | What opportunities do you see for your business with the increasing digitalisation of energy networks? |
| 2 | What are your main concerns with the digitalisation of energy networks? |
| 3 | What are the technical and organisational barriers to integrating cybersecurity into your organisations? |
| 4 | What do you see as the top risks or things that could go wrong with IP connected infrastructures? |
| 5 | What special requirements do you have for solutions to be applicable to an always on operational setting? |
| 6 | Do you have specific concerns related to adapting IT approaches to OT settings? |
| 7 | Can you identify some enabling technologies or functions that may require development or testing to be ready for deployment? |
| 8 | What do you see as the key challenges in defending the energy infrastructure attack surface? |

Table 3 Energy Cybersecurity Question Set

The main findings were reported by each group. The arising issues were then discussed as a whole workshop group and categorised into emerging themes that are outlined in Section 5.2.

This practice space provided a learning platform, taking participants beyond their current skill area. There is evidence of bias towards skill areas in the workshop discussions, for example in Section 5.2.1 there were different views on the necessity of encryption coming from participants with IT and OT backgrounds where latency requirements could render encryption to be inappropriate for grid protection safety mechanisms, where the context of high voltages speaks louder than confidentiality of communications. The workshop discussions were building a shared understanding of the OT context with participants.

### 2.4.2 Industry Interviews

A cross-check of the emerging themes was carried out with other group facilitators from the workshop. To then add further perspectives to the picture and build on the findings of the workshop, some follow-up interviews were carried out with each of the participating organisations. These interviews were conducted in a semi-structured manner to check understanding of workshop outputs and to allow further sharing beyond what could be communicated in the group workshop setting. The base question set in Table 3 was revisited with PNDC members who had not been able to attend the workshop, and further discussions of the themes that arose during the workshop were facilitated through open questioning. Table *11* in Section 4.1 summarises the resulting set of issues that were common to all the DNOs.

The synthesis of different knowledge areas, achieved through the workshop and interviews, was to inform and communicate the needs of OT and improve understanding of the operational context for cybersecurity implementations.

## 2.5 Developing beyond ISAC information sharing

This stage of the research provides an illustration of implementing a common vision of cybersecurity improvement across a community of actors. It utilizes a collaborative framework that has facilitated the co-production of cyber security guidance for energy sector participants. It addresses the gaps identified in previous literature (in Section 2.8) by providing a contextual study of co-producing cybersecurity guidance with an energy sector

community, and by enabling a more integrated cyber capability across different energy sector actors.

### 2.5.1 Survey of NIS Experiences

The EE-ISAC created an opportunity and platform for information sharing between the public and private sector with, in some situations, the ability to meet the needs of both. An example of this was an investigation of challenges related to the implementation of the NIS Directive in the energy sector. This was carried out by inviting energy operators, in EE-ISAC's membership and wider network, to share their experiences in implementing the EU Directive on Network and Information Security (NIS) during its first year. Due to the sensitivity of sharing information, the survey offered the chance to give anonymous feedback to the NIS Cooperation Group. The sharing was enabled by using an anonymous space and by combining the feedback, thus achieving the benefits of collaboration while also addressing the need to protect information [14]. A set of open questions were used to gather feedback from energy operators.

### 2.5.2 Survey of Energy Operators

A full set of open questions were offered to elicit feedback and encourage a thorough response from Energy Operators on their experiences with implementing the NIS Directive. The questions were made available to both EE-ISAC members and their non-member contacts, for a wider representation of energy operators in the responses collected. The actual list of questions used are listed in Table 4. The questions were reviewed by the EE-ISAC Board and by a representative from ENISA before energy operators were invited to submit their responses.

| | |
|---|---|
| 1. | Is the NIS Directive published guidance adequate? |
| 2. | Is the criteria for identifying an Operator of Essential Services clear and transparent? |
| 3. | Please comment on the challenges in achieving a clear picture of the latest cyber security issues? |
| 4. | Are available threat intelligence sources sufficient to decide and prioritise actions? |
| 5. | Are there any concerns with the effectiveness of risk assessments and risk management systems? |
| 6. | Are there any issues with the identification of interdependencies, cross-sector and intra-sector or cross border? |

| | |
|---|---|
| 7. | Please comment on the ability of relevant stakeholders to cooperate and collaborate and achieve clarity with crisis management procedures? |
| 8. | Describe the current challenges in achieving compliance through supply chains? |
| 9. | Are there any difficulties with establishing networks for incident response? |
| 10. | Any challenges with achieving both the technical and human capacity to address the issues? |
| 11. | Please comment on the clarity of reporting thresholds and national notification schemes? |
| 12. | What other challenges do you face when deploying cybersecurity solutions? |
| 13. | Any comments on the incentives for investing in security? |
| 14. | Please comment on the clarity of security measures in compliance monitoring frameworks? and any issues you see with defining security standards? |
| 15. | Any comments on the application of the NIS Directive in different countries, especially for multi-national companies? |
| 16. | Would you like to share any other feedback or challenges with applying the NIS Directive to your situation? |
| 17. | Do you have any additional comments related to Public-Private Cooperation in securing the energy sector? |

Table 4 Survey Questions

### 2.5.3 Integrating knowledge

Initially, time was given to support the building of a trusted network and to establish the culture of information sharing as a central activity of the group. To then take this information sharing towards improved outcomes in cybersecurity, the practice group approach described in Section 2.1 was applied to launch practice spaces on specific topics. This was done for Risk Management and Incident Response, to integrate knowledge and experience and co-produce more useable information, resulting in white papers to be shared more widely as guidance for the energy sector OT community. Meetings were held to discuss a framework for the topic. Each participant provided some input, which was reviewed by all. The sharing and synthesis of skills and knowledge provided learning for the participants, and for the sector by bringing together the information into one useable reference document.

In this manner, a synthesis of different risk research brought the work closer to potential users. Similarly, a synthesis of IT and OT expertise enabled incident response guidance to be produced for an OT energy context. This became an integral part of the ISAC culture,

normalised as what we do, and the group later worked together to combine their experience into a living document on threat intelligence to share new approaches over time.

### 2.5.4 Trusted Hub for Grid participants

A reflection session with members provides a picture of the progress of the ISAC described in Section 7.1. From the author's central role within the ISAC and study of the evolution of information sharing, across ISAC activities, NIS interventions, and Network Code developments, the author provides an analysis of the current position of EE-ISAC, and proposes a trusted hub for collaboration across the synchronous grid area that is presented in Section 4.2.1. and Section 7.5.1., and additionally recommends future focus areas for the ISAC in Section 4.2.2 and Section 7.6.

## 2.6 Supply Chain Shared Responsibility

Significant concerns around the cybersecurity of supply chains were raised by both the PNDC and ISAC practice groups. The third stage of this research therefore focusses on the Supply Chain challenge area, to further investigate interorganisational workings, exploring from both within and beyond the energy sector.

While regulatory frameworks incentivize individual organizations to improve their cybersecurity, operational services contain contributions from many organizations and this supply chain of activity needs to be influenced and managed to achieve desired security outcomes. Operators of critical infrastructure hold responsibility for the impact of cybersecurity events in their operational environment and on the essential services they provide. Regulatory frameworks such as the Security of Network & Information Systems (NIS Regulations) in the UK [15] and the European NIS Directive [16] place cybersecurity expectations on individual organizations but the operational services deployed utilize components, products and services coming from multiple supplier companies. Dividing up cybersecurity responsibilities and transferring risk between organizations and between customers and suppliers proves to be a challenge. As a result, regulators further propose to broaden the application of NIS Regulations to organizations supplying to critical infrastructure services [17] [18] [19]. Although, these regulatory tools can only focus on the cybersecurity obligations of individual organizations, rather than defining end to end security for the technical solutions and services that encompass multiple actors.

### 2.6.1 Analysis of Perspectives

The author carried out interviews with organisations in the Energy, Water and Transport sectors, including semi-structured interviews with Operators of Essential Services (OES) and Competent Authorities (CA) in those sectors, as well as meeting with NCSC and lead Government departments, to assess the progress of the NIS Directive. The experiences of each of the roles and responsibilities supporting the implementation of the NIS Directive were included. This enabled the challenges to be understood from the different perspectives of providers of essential services, their suppliers and regulators. Due to the sensitivity of the topic and to investigate different approaches being used, and identify the barriers to progress, semi-structured interviews and discussions captured the different viewpoints.

To advance academic contribution while also enhancing practical progress, this work included some action-based research to assist stakeholders in meeting their objectives under NIS and progress cooperative partnerships in cybersecurity. The author participated in industry collaborations and working groups that were formulated to progress the supply chain resilience effort. This assisted in building trust with interviewees due to the sensitive nature of cybersecurity.

The names of organisations and participants in the research are not disclosed for confidentiality and anonymity reasons. To draw on the direct experience of operators implementing their NIS obligations and suppliers impacted by NIS, as well as Government guidance and oversight, the spread of participants were as indicated in Table *5*.

| **Private Sector Participants & Roles** | **Public Sector Participants & Roles** |
|---|---|
| **OES** (15 participants) | **Government Technical Advisory** (5 participants) |
| Head of Digital Security | Incident Management |
| Director of IT | Product Assurance |
| IS Security | Project Manager Cyber Exercises |
| Data Protection Specialist | CNI Team, Sector Leads |
| Information Security Officer | Sociotechnical Security Group |
| Cyber Risk & Compliance Manager | |
| OT Systems Managers | |

| | |
|---|---|
| **Suppliers** (7 participants) | **Government Policymakers** (5 participants) |
| Solutions Architect | Cyber Resilience Policy Advisor |
| Systems Integrator | Policy Advisor, Cyber Incentives and Regulation |
| Cybersecurity Business Lead | Cybersecurity Regulatory Policy |
| Product Solutions and Security Officer | Cyber Resilience Policy Advisor |
| General Manager | Cyber Policy Team |
| | |
| **Sector Collaborations** (4 participants) | **Competent Authority** (8 participants) |
| Chair of Industry Supplier Assurance Working Group | Cybersecurity Oversight Specialist |
| Industry Association Members | Network Security Director |
| | Cyber R&D Lead |
| | Inspector |
| | Specialist Inspector |
| | Regulation & Governance |
| | Sector Head of NIS |
| **Consultants** (3 participants) | **EU Participants** (4 participants) |
| Cybersecurity Consultant | Information Security Expert |
| Digital & Data Consultant | Secure Infrastructure & Services |
| Principal Cyber Consultant | NIS Stakeholder Reviews |

Table 5 Summary of Research Participants

The main topics of questioning during the interviews included a participant's overall experience with implementing NIS; their interaction with the supply chain and ability to control and manage it; and their processes and approach to NIS and managing suppliers. The following tables show the list of questions that were used to facilitate discussion of the problem area with OES, Suppliers and Competent Authorities from each sector. Discussions with other government actors, such as NCSC and policymakers, included reporting back and discussing their perspectives on the findings. Table *6* shows the areas of interest and questions posed to operators.

| | **Supply Chain Questions for OES** |
|---|---|
| General questions: | |
| 1 | What is your overall experience of implementing NIS? |

| | |
|---|---|
| 2 | How has NIS impacted your organisation, has it helped you? |
| 3 | Can you describe your efforts to implement NIS expectations into OT areas. |
| Boundaries of action: | |
| 4 | How far are you able to control and manage the cybersecurity of your supply chain? |
| Guidance: | |
| 5 | Is the guidance in your sector, such as the CAF, clear and detailed enough for your organisation to achieve NIS compliance? |
| Managing the Risks: | |
| 6 | What process is being used to identify and manage risks in the supply chain? |
| 7 | How does the management of suppliers align with your organisations' risk appetite? |
| 8 | How do you manage suppliers differently where they might have different levels of importance to you? |
| Procurement: | |
| 9 | How do you include cybersecurity in your procurement and selection of suppliers? |
| 10 | How do you communicate your cybersecurity requirements to suppliers? |
| Accountability and Responsibilities: | |
| 11 | How are you passing on your NIS obligations to your supply chain? |
| 12 | Are you transferring risk to your suppliers? or sharing responsibilities? |
| 13 | Are you auditing suppliers or relying on self-assessment? |
| Contractual Agreements: | |
| 14 | To what extent do your contractual arrangements with suppliers include cybersecurity or assist your compliance with NIS? |
| 15 | How are contractual agreements with suppliers meeting the latest operational issues? Are operational realities reflected at a contractual level? |
| | Processes: |
| 16 | How do you manage people and equipment with access to Operational Technology? |
| 17 | How do you ensure compliance of suppliers with your security policies? |
| 18 | Is cybersecurity training and awareness being extended to appropriate parts of the supply chain? |

| | |
|---|---|
| 19 | What visibility do you have of cybersecurity practices in lower tiers of your supply chain, how do you ensure sub-contractors are complying with your security policies? |
| Threat Intelligence: | |
| 20 | How is threat intelligence shared with your supply chain? Is there expectation on suppliers to communicate new threats and vulnerabilities? |
| Incident Response: | |
| 21 | Are appropriate suppliers engaged in and aware of your incident response plans and business continuity plans? Is support during incidents included in agreements with suppliers? |
| 22 | Can you describe the effectiveness of your relations with suppliers during incidents, while risk assessing new vulnerabilities, or managing software updates etc.? |
| | Performance: |
| 23 | What are the costs and benefits to your organization of investing time, money, and effort into securing the supply chain? |
| | Cooperation: |
| 24 | To what extent do you work together with other OES in your sector eg sharing cybersecurity best practices? |

Table 6 Supply Chain Questions for OES

Some of the Table *6* questions were also used during interviews with the competent authorities to understand, from their audit & compliance visits, the CA perspective on what had been achieved by OES. The main question set for competent authorities related to their role in NIS and are listed in Table *7*.

| | **NIS Oversight Questions for CA** |
|---|---|
| 1 | How are you overseeing the supply chain security aspect of NIS? |
| 2 | What are your expectations of OES in terms of being in control of the cybersecurity of their supply chains? |
| 3 | How do you prioritise which OES to audit? |
| 4 | Are there challenges in terms of skillsets required to audit OT and ICS facilities? |
| 5 | How are you setting expectations on OES or identifying priority areas to focus on? |

| | |
|---|---|
| 6 | How is the scope of NIS being decided and agreed for each OES? |
| 7 | Do you monitor the actual suppliers OES are using and how do you act on this information? |

Table 7 Questions on oversight of NIS for CA

Table *8* lists the questions asked of supplier companies to CNI.

| | **Questions for Suppliers** |
|---|---|
| 1 | How are the NIS obligations of your customers being communicated to you? |
| 2 | Is it clear to you what cybersecurity requirements you are required to meet, for each customer or for a sector? |
| 3 | At what stage in the procurement lifecycle are cybersecurity expectations presented to you? |
| 4 | Are security initiatives being driven by OES needs or by your security offering? |
| 5 | Is your cybersecurity capability prioritised during procurement i.e. does your security maturity level give you an advantage in the current market? |
| 6 | Is your security capability being effectively utilised by OES? |

Table 8 Questions for suppliers to CNI

## 2.7 Validation

This research was continually validated at regular intervals through interactions with the industry sponsors of the Future Power Network and Smart Grids Centre for Doctoral Training (CDT), through active participation in public-private partnerships, and through cybersecurity projects with industry partners at the PNDC.

Furthermore, this research facilitated the coming together of different experiences and understandings, such as IT skills adapting to an Operational Technology (OT) context and a synthesis of power systems and telecoms experience. This research involved bringing together different experiences to make clear the context of a changing energy sector. The changing role of Distribution Network Operators (DNO) was also considered as they evolve to include system operator responsibilities to balance power flows for their grid zones.

## 2.8 Related Works

The following sections place this thesis within the context of related works.

### 2.8.1 Practice spaces and multi-actor approaches

This research was inspired by the following works on forming communities of practice for different areas of expertise to work together and on creating new knowledge from a synthesis of disciplines.

Listening, understanding and valuing the security dynamic as a process within a particular context, Gjorv argues for multi-actor approaches to security that encompass the dynamics between public and private actors in the creation of security [20].

Galafassi's social ecological knowledge co-creation included sharing experiences, connecting perspectives, and finding applicable knowledge & methods to design interventions [21].

Anderson introduces a 'Third Space' to open up new possibilities 'between and beyond', a place for being creatively open to redefinition and new directions. Stepping into a third space was required to respond to changing contexts, and to facilitate new insights [22]. The practice spaces during the author's research all provided a third space to facilitate new insights and design new approaches by co-constructing new knowledge.

Hulme co-constructs trans-professional knowledge for school settings aiming towards a joined-up service provision, by evidencing progress where practitioners 'own' the emergent forms of trans-professional knowledge. Working in integrated contexts requires 'new forms of collaborative working and a commitment to the co-construction of knowledge' [23]

Scharmer introduces the concept of not-yet-embodied knowledge as a pathway to tap into emerging business opportunities. This requires a space or platform to transit away from current practices towards new ways of working; being in front of a blank canvas, together, in a process of shared will, shared reflection and shared action [24].

The trans-professional and transdisciplinary aspect of the author's research included the four phases identified by Hall [25] as providing efficient processes that can leverage effective outcomes:

1. Development – establishes the foundation for integrative knowledge creation.
2. Conceptualisation – collaboration to develop research questions and conceptual model for the transdisciplinary endeavour.
3. Implementation - progressing towards practical solutions.

4. Translation - of research findings into practice and application, towards solving real world problems. [25]

### 2.8.2 Defining the new energy context

The author's research builds upon Hurst's work that recommended a holistic defence in depth approach after surveying different infrastructure security strategies. Proactive protection needs a broad view of the infrastructure, coordinated responses to disruptions and requires diverse information about systems, networks, devices and processes to model correct behaviour [26]. The research combined insights from several sources including literature, relevant project experience and analysis of discussions [27]. Interactions during the workshop and the experience of participants enabled the building of the analysis and the discovery of the categories. Interviews allowed time to further explore with in-depth discussion, using open questioning based on the themes and categories that arose during the workshop.

The context picture was constructed through interaction with the field. This work was constructivist [28] due to the collaborative engagement to build knowledge, involving interactions with participants' prior experience in their field and closeness to the situation, especially where their roles included responsibility for cybersecurity or operational facilities. Bringing together stakeholders in this way to address sector specific issues with mutual cooperation and by going beyond organisational boundaries also aligns with Burns' partnership approach [14]. A multi-actor approach by listening and understanding different perspectives across industry was paramount to this research [20].

### 2.8.3 Beyond information sharing

Messenger [29] [30] researches the cultural dynamics at play with sharing of cybersecurity information across organizational boundaries and proposes the following model of beliefs that are necessary for sharing cybersecurity information:

- I know that my information is important and urgent.
- I know that what I share will help others.
- I know I am trusted by my organization.
- I know how to get the information to the right people.
- I know I can control what happens with what I share.

- I know others will all act with my interests at heart.
- I know others will reciprocate.
- I know I am empowered to share. [30]

The work of this thesis aligns with Borchert's recommendation to go beyond information sharing and to actively co-produce content together [31]. Rather than information sharing between parties, Borchert recommends joint information ownership and co-production, involving relevant stakeholders by providing a framework to engage them, fostering good relations and trust, and a dedicated focus on developing content together, ideally setting up information co-production per sector to address specifics [31]. Borchert recommends stakeholders co-produce information together, moving beyond information sharing between organisations to shared ownership of information. This would aim to provide actionable information for tackling immediate threats and improve understanding of the broader context of unfolding developments and future risks. The need to organise information flows between stakeholders necessitates a process-based approach, to improve preparations and continuously adapt to a changing security environment [31].

The field-based approach to this research and the participant observation carried out during the development of the EE-ISAC aligns with Whyte's research method [32]. While being on the scene and sensing the importance of the events, it became possible to create "solid description and analysis" from a place of participant observation. Realising the significance of having a central role from which to provide insight, through both record keeping of formal meetings and experiences of informal discussion [32]. Actions taken included bringing together stakeholders to a roundtable setting to address sector specific issues with mutual cooperation and expanding beyond organisational and national borders [14]. The use of anonymity, where stakeholders were less willing to share sensitive information, provided a platform for gathering and analysing information anonymously and then acting on it collectively [14].

Listening and understanding different perspectives across government and industry was paramount to this research. Gjørv recognises researchers as playing a direct part in the securitisation process by listening and understanding security from their professional field and by being "acknowledged as part of the process". Gjørv recommends "more visible and concrete engagement between actors" and understanding their security practices and

assessing and valuing the security dynamic as a process within a particular context. Both the subjective and objective engagement of researchers in security as a negotiation between actors, seeing the context-based needs of actors, “the extent to which trust is present” and facilitating the inclusivity of different perspectives [20].

### 2.8.4 Securing Supply Chains

Due to cybersecurity continually evolving, it became important to involve industry practitioners and include perspectives of different stakeholders for a deeper understanding of the dynamics of the OT context. In this respect the author’s work aligns with Stringer’s action research bringing change to communities, with its emphasis on collaboratively constructed interpretations, providing the opportunity for the work to adapt to particular environments for mutually acceptable solutions that more effectively deal with the problems [12].

Kumar’s research on the impact of cybersecurity on operations identifies a critical need for companies to develop a strategy to secure their global supply chains [33]. Ghadge identifies generic research into supply chain cybersecurity and points out the need for more contextualized studies in specific domains [34]. Melnyk calls for more research into cybersecurity across the supply chain and highlights the importance of alignment to a common vision in both a vertical plane, through various actors within an organization agreeing on common goals for cybersecurity, and through horizontal alignment across inter-dependent organizations working together on common cybersecurity objectives [35].
Shaked et al captures expressions of cyber resilience in the constituents of a sector and in the relationships between them, and recommends coordinating cyber resilience across a system’s constituents rather than relying on self-evaluation by individual entities [36]. Kroger recommends that processes transcend existing organizational boundaries and follow an “all actors approach” to address the multi-faceted risks of critical infrastructures more holistically [37].

Sitton & Reich [38] compares systems engineering methods for improving interoperability across enterprises where existing assets and systems have been developed at different times and places leading to a lack of synchronization. The integration of complex emergent systems is considered from a process design perspective, presenting cross-enterprise processes and

information flow as being key to seeing the broader view necessary to lead the way from uncoordinated unsynchronized systems and domains towards new integrated capabilities at the processes level. This tends to be hindered by there being no allocated responsibility for defining operational process requirements across organizations. Sitton & Reich therefore recommend viewing 'both ends' by combining a top-down strategic thinking and standardization across organizations with a bottom-up evaluation of a continuously evolving environment. Their research calls for future projects to demonstrate the planning and management of operational processes to achieve integrated capabilities for complex emergent communities. [38] The author's research, and guidance co-produced in the author's practice spaces, has achieved some steps towards this that are now being progressed further through impact activities.

# 3 Background - securing a changing system

This chapter provides some background information on the evolving energy system and the increasing need for cybersecurity vigilance, including an example of a targeted cyber-attack.

Joining together a communications and control infrastructure with the power system introduces new risks and increases the potential attack surface. The field of cyber security is very broad, and within large organisations such as Distribution Network Operators (DNO), often operates at different levels of abstraction, from board and management level, to policy and procedure creation, down to product-level security of equipment being installed, as well as deeper into the specific workings of individual devices installed on a network. Cybersecurity is an important topic for DNOs, since attacks may adversely affect assets, or result in outages and customer minutes lost, or present safety risks if control of the network is available to an unauthorised party.

The power system is made up of a range of interoperable architectures, each being owned and operated by different parties. The reality of having multiple responsible entities is a more fractured configuration that can lead to gaps in security. Figure 4 implies that while different departments and suppliers are arranging their own cyber security implementations, such disparate solutions may not combine to offer acceptable end-to-end security.

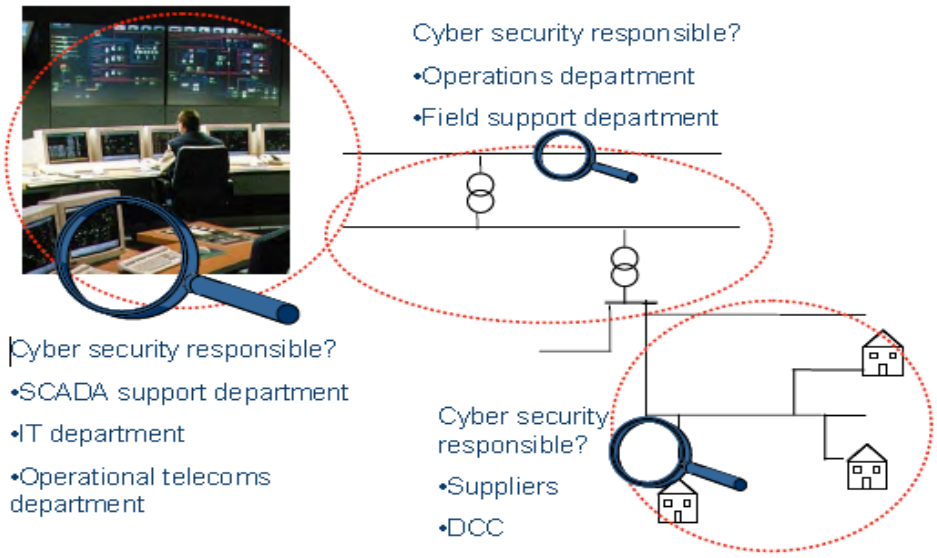


*Figure 4 Secure areas with potentially disparate solutions* [39]

To ensure all aspects of cyber responsibility are covered end to end, a more holistic security management is needed. The energy system requires an end-to-end security capability working *consistently* across organisational boundaries and throughout the entire distributed system, see Figure 5.

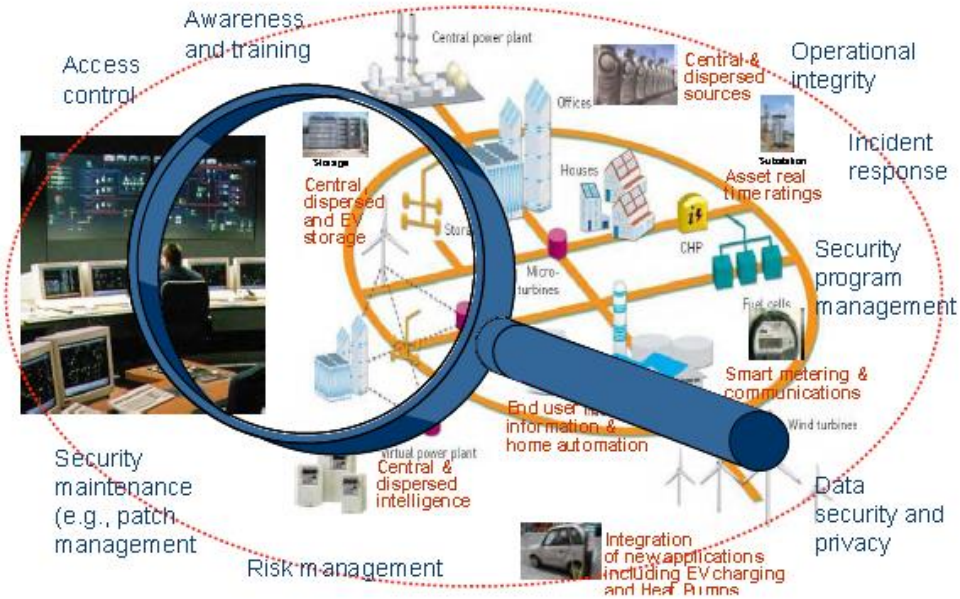


*Figure 5 Holistic end-to-end security* [39]

A clearer understanding of the impact of potential security incidents on the system would allow strategic decisions around risk to be made to determine where to implement and update security controls and technologies. A better understanding of the risks can identify appropriate security requirements, whether encryption and authentication are required or additional measures, such as packet inspection of data content, are necessary to manage threats in a cost-effective manner.

## 3.1 Increasing Risk to Distribution Networks

Modern electricity networks include electricity markets to facilitate the trading and supply of electricity from generator to customer. The primary players are:

- Transmission System Operator (TSO) in charge of operating, managing, and maintaining the high-voltage transmission network.

- Distribution Network Operator (DNO) responsible for maintaining and operating the lower voltage distribution networks. The role of the DNO is evolving from a traditional 'fit-and-forget' model to a more active role resembling the responsibilities of the system operator, identified as a DSO.
- Generators providing energy with contracts in place to guarantee certain amounts of power.
- Customers as domestic, business or industrial consumers of electricity.

New arrangements between TSOs and DSOs with more distributed responsibilities to balance supply and demand of electricity are bringing new uncertainties, new roles and communication channels that requires an effective integration of tools and processes.

There is a rapid increase in connected devices underway for the distribution layer. Distribution networks contain embedded devices that typically have no mechanism for the end user to install security software onto them. The security of these devices is therefore dependent on the device manufacturer. Even with security capability for endpoints, networks and data, it is very difficult to implement them everywhere. Also, in many cases security controls would need to be implemented by vendors themselves. Table *9* outlines some possible security breaches that would affect Availability, Integrity and Confidentiality (AIC) and gives ideas of counter measures that could be taken to minimise the impact.

| | **Potential impact of not achieving AIC** | **Examples of Counter measures** [40] |
|---|---|---|
| A Availability | Devices unreacheable due to denial-of-service attack flooding communications network.<br>Malicious users accessing control systems and causing power outages such as remote operation of circuit breakers, triggering smart meter load drop, ANM curtailing generation.<br>Cascading failures across the grid, through directing sudden load or generation losses. | Islanding.<br>Local control<br>Distributed communication servers. |

| | | |
|---|---|---|
| I Integrity | Injecting data to change behaviour of devices<br>Changing data so incorrect decisions made by control units<br>Manipulation of synchro-phasor readings to cause load shed.<br>Customer bill 10x higher | Use local sensor info to validate control commands.<br>Detection of false measurement or control data. |
| C Confidentiality | Invasion of privacy from observing appliance use.<br>Theft of customer data.<br>Obtaining credentials for control system access. | Preventing malware infection. |

Table 9 Potential impacts of security breaches and suggested counter measures

It is a challenge to keep updating systems to mitigate against new threats in an operational environment where availability is paramount. Preventative measures such as system updates and modifications, require testing before going live, and are often not feasible until an outage of the asset happens. If availability is expected to be at say 99% but we have inadvertently designed an opportunity for adversaries to take control of many devices, then the risk that they will take up that opportunity and cause availability to drop could be high. In addition, workforce availability for other activities is affected if they are dealing with targeted attacks on critical systems.

## 3.2 Cascading Effects

Cascading effects are when failures propagate to cause extensive blackouts across the power grid. The cyber infrastructure offers greater visibility and a decision support tool to assist in preventing failures from cascading, however cyber security issues can introduce another potential trigger for cascading effects and increase the risks of blackouts occurring.

The “undesirable and unnecessary operations of protective relays during power system disturbances have contributed to many cascading power failures” [41]. Relays have been pre-programmed with responses to changing local conditions. Despite operating as intended, their combined response “can create unrecoverable instability in the power system” [41]. It is essential to system reliability for control systems to coordinate these

protection devices but in a cyber secure way. Wider area controls could coordinate a more adaptive response with the potential to create a stable configuration of system islands and prevent cascading failures. A significant power outage in the UK in August 2019 emphasised the importance of adaptability and cooperation in operating a changing and complex power system [42].

## 3.3 Reliability

"Only very reliable intelligent control can improve an already reliable physical infrastructure" [43]. Utilities traditionally have demonstrated a culture of high resilience through creating N-1 reliability across the transmission network. Reliability studies are likely to paint a different picture if analysed across the power and ICT infrastructures combined. The grid tends to be operated like two separate systems, the demand side including the distribution network, and the supply side including the transmission network. Reliability is handled differently for each [44].

### 3.3.1 Supply Side Reliability

On the supply side the focus is on achieving security of supply and having additional generation capacity above peak demand available in reserve. The risk of customer disconnections is assessed using Loss of Load Expectation (LOLE). This is the average number of hours per year when there is insufficient supply available to meet demand. The challenges involved in achieving security of supply include:

- Projecting future demand
- Generation availability
- Interconnectors able to respond when needed
- Wind resource availability
- Impact of weather on demand profile [45].

The transmission network is regulated by an input standard that specifies network planning must include a contingency of N-1. There is emphasis on having back up in place for generation and the transmission network. Where several transmission lines are feeding a load point, if one of those lines, even the highest capacity line, goes out of service then the remaining lines must continue to supply the full load. Likewise, the system must still be able to meet demand when one generator is lost, even if it is the biggest generation plant on the system.

### 3.3.2 Demand Side Reliability

The distribution networks are regulated by reliability standards that incentivise keeping service interruptions to a minimum. Financial penalties are enforced for Customer Interruptions (CI) and Customer Minutes Lost (CML). These are derived from the average number of interruptions per customer and the average outage time per year. However, not all outages are included because adjustments can be requested. Severe weather events that exceed 8 times the daily average high voltage (HV) fault rate for the last years are excluded from the penalties. One-off exceptional events are also excluded that involve >25,000 interrupted customers or >2,000,000 interrupted minutes [46].

Some regulators in other countries have different approaches to deciding what interruptions to exclude from reliability metrics. The regulator in California believes that reliability should not be measuring “a world without any disturbance” and believes the metrics must “reflect the actual responsiveness of the distributor in addressing disturbances” [46].

Reliability may require a different approach going forward. Consider the consequences of increasing complexity. A smart grid is more complex than a physical grid and each component adds another potential source of failure to the system. While increasing intelligence within the grid is helping reliability by introducing more control capability, each layer of complexity also introduces new interdependencies and attack surfaces. The overall reliability of the system is a function of the reliability of each element, including both physical and cyber elements [43].

Reliability has so far been strongly built into the system to ensure supply meets demand. For this reliability to remain at its intended level in a smarter grid, we would be relying on adversaries *not* taking up the opportunities a more connected system offers them. Security is overlaying a whole new set of concerns. The demand side could be more at risk of service interruptions than the supply side, due to its distributed nature and it now including generation as well.

## 3.4 Holistic thinking

Security solutions need to be updateable and adaptable to future exposures. It is not about protecting a static infrastructure, “the reality is a dynamic, fluid environment” [47]. Many common threats can be addressed by applying available security tools and defence tactics. It is the adaptive, embedded and interconnected threats that can only be addressed by a well-developed workforce [47]who are supported by a whole systems approach to secure operations. While there is a need for convergent thinking, looking into the security issues with each component to develop the necessary tools to secure parts of the system. There is also a need for divergent thinking looking at how the component parts will work together to synthesise the working principles required to secure the operational space. This could include setting up the cycles of learning that are essential for security improvements and the purpose and direction that keeps operations performing well even during incident response [48].

## 3.5 Consequences & Impact

Probabilistic methods can be used to improve the assessment of risks. The risk to the system will be made up of the likelihood of a particular threat and its potential impact. When considering impact, it is necessary to look beyond individual components of a system to the interconnections and relationships between them, so the full impact across the whole system is understood. Looking at individual issues in isolation could result in gaps or unintended consequences. Considering the causal relationships between issues and how elements of the system interact is likely to allow a more thorough picture of the impact to emerge so that security can be addressed more effectively with a better appreciation for where security improvements are needed most. Inspired by Pearce’s Issues Framework, for a context driven appraisal of multiple factors affecting sustainability used to support decisions and balance a complex set of issues. The author produced the issues wheel in Figure 6 to orient around the full list of stakeholders and areas to consider. This could be further developed in future work, alongside resilience measures, as a gauge to assess the response of the system to the latest threat landscape and see the full impact across all layers of stakeholders and system components [49].

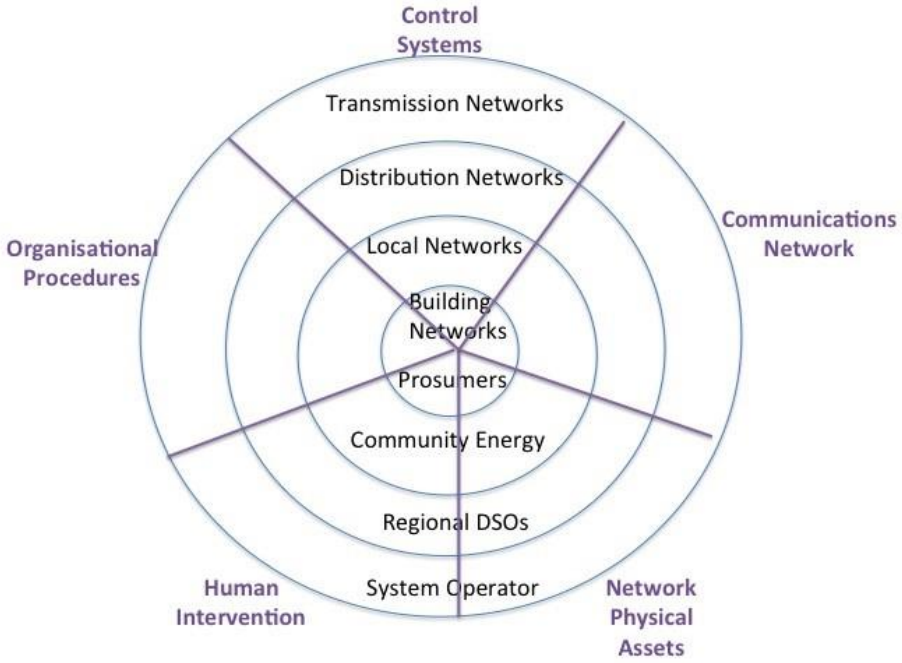


*Figure 6 Issues Wheel*

## 3.6 Cyber Attacks on the Power System

### 3.6.1 Advanced threats

While existing cyber security guidelines have encouraged progress with securing networks from nontargeted attacks, not all threats can be prevented. Determined adversaries with resources and competencies to create targeted attacks can bypass most security controls. As well as prevention there needs to also be preparation of a planned response for when adversaries gain access to critical systems. If our most important systems are increasingly being penetrated by unauthorised actors then additional steps need to be taken, such as obfuscating high-priority targets, to deal with inevitable attacks [50].

The solution requires investment in people and processes, not just technology. Research by CGI has recommended the following as the highest priority areas to be focussing on:

1. Security Awareness
2. Security Training
3. Governance – meeting Security Requirements, assessing Risks
4. Advanced Threat Monitoring
5. Managed Security Services [51].

A thorough, combined approach to protecting our energy systems will include people, by considering human factors; technology, through implementing appropriate security tools; and procedures that encourage cyber security awareness and enable incident response.

### 3.6.2 Ukraine incident

In December 2015, three power distribution companies in Ukraine experienced remote cyber intrusions that impacted multiple central and regional facilities. The synchronised and coordinated attack caused power outages to 255,000 customers. While power to customers was restored within 6 hours, the attacks left a lasting impact such that all three distribution companies were still running under constrained operations several months after the attack [52].

It appears the attacks were planned several months in advance due to malware infections delivered through phishing emails to employee email accounts. The emails asked employees to click on "enable content" to read an attached document. This loaded Black Energy attack software onto their office computer systems which established a line of communication for the attackers to spend time looking for passwords, gathering an inventory of systems, and searching for ways into the operations and control room systems from the business computers they already had links into. Black Energy has been reported as one component that enabled access, there could have been other methods used as well. Some additional runs of spear phishing emails also helped them to discover log in details for the operating systems. The malware enabled legitimate credentials to be acquired to facilitate the remote operation of circuit breakers. Operators saw cursors moving across their operating screens to trigger the blackouts but they were locked out of the system because attackers had changed the passwords so the operators could not take back control [53].

The attacks appeared to be coordinated by multiple external actors based on the timing of events shown in Table *10*.

| **Timing of event** | **Attack event** |
|---|---|
| 3.30pm | Power outages at 1st utility |
| 3.31pm | Power outages at 2nd utility |
| 4.06 pm | Power outages at 3rd utility |

| | |
|---|---|
| 5pm | Denial of service attack on call centre prevents customers from reporting problems. |
| 6pm | Hackers cut off back up power source to an operator's control centre. This prevented their systems from rebooting so they had no visibility of unfolding events. |
| 9.30pm | All power restored by switching to manual controls. |

Table 10 Sequence of Ukraine cyber attack [54]

To interfere with restoration efforts, several activities were carried out by the attackers to cause some ongoing impact for the distribution network operators. A Denial-of-Service attack on the call centre was carried out to prevent customers from being able to report the power outages. Devices at substations were rendered inoperable by corrupting their firmware. Some systems were wiped by executing KillDisk malware: Windows based Human Machine Interfaces (HMI) embedded in Remote Terminal Units (RTU) were overwritten with KillDisk. The Uninterruptible Power Supply (UPS) remote management interface was used to schedule disconnects [55].

Ukraine power distribution companies are still able to operate their networks manually so the outages to customers were only experienced on the day of the attack. This sort of attack would have caused a bigger impact for power companies that have replaced their manual operations capability with newer technologies [56]. A greater reliance on automation would have resulted in a more prolonged blackout [57].

### 3.6.3 Restoring trust

The Ukraine experience has demonstrated a loss of trust in their devices and control systems, with manual operation still going after several months. Recovery from a cyber-attack is different to recovery from a natural disaster when cyber-attacks can leave active malware hidden and undetected inside power systems. The attackers had learnt three different power distribution management systems at three different power companies in order to carry out the attack.

Traditionally, distributed devices trust commands received from the control room. In the Ukraine attack, the system carried out the hackers' commands without question. It was not programmed to notice if many users simultaneously log in from unusual internet

protocol addresses. The system was unable to notice that it was being requested to open high-voltage circuit breakers at dozens of substations [53]. When grid operations are smart under normal operations to take advantage of the benefits offered by greater intelligence in the system; they must also remain 'smart' when under attack. This will require intrinsic safety and security measures that preserve critical operations with procedural or technical workarounds. Systems need to be more robust to expected failures and able to recover from unknown failures. Rather than broad general rules applied by central control, this may require more flexible subsystems able to discover their local situation by operating with awareness of the behaviour of other components.

# 4 Research Outputs

The research outputs of this thesis are summarised here and detailed in the later sections.

## 4.1 The Energy Context Key Research Findings

This work is published in the following reference and was presented to the Energy Networks Association and also at ESORICS 2021 Workshop:

Tania Wallis, Greig Paul, and James Irvine, "Organisational Contexts of Energy Cybersecurity," Conference Proceedings SPOSE2021 at ESORICS. Lecture Notes in Computer Science, vol 13106. Springer. doi.org/10.1007/978-3-030-95484-0_22.

This work was carried out ahead of the NIS Directive being enforced, before cybersecurity regulations were imposed on operators of essential services. At this point, from an industry perspective, cybersecurity was a new consideration for operational networks that had previously not been connected to the internet. From an academia perspective, this work happened alongside the launch of a new research theme at the PNDC that was opening a door for new specialties coming from communications and cybersecurity into an area of power networks expertise. This work formulated the mental models of what was through this 'door' and the considerations that cybersecurity deployments would need to integrate with to be effective in future energy network operational contexts.

Table 11 outlines the key areas of concern raised by workshop and interview participants.

| **Key Areas of Concern for DNO Organisations** | |
|---|---|
| Access Control | Local, remote access.<br>Operator, 3rd party, corporate users.<br>Always-on environment.<br>Automated actions without users.<br>Logging and monitoring.<br>Timing of measurement & authentication. |
| Updates | Authenticating remote updates.<br>Updating working equipment in the field.<br>Use of whitelisting to ensure only original software able to execute. |
| Network Monitoring | Identify unusual traffic.<br>Visibility of devices. |

| | |
|---|---|
| | Log aggregation.<br>Limited bandwidth to remote sites.<br>Distributed trust to authorise communications. |
| Legacy Systems | Identify devices.<br>Apply network segmentation.<br>Monitor configuration events.<br>Identify suspicious access or traffic.<br>Lifetime of vendor support.<br>Consider wider engineering solution, beyond the security solutions, especially where there are security gaps. |
| Culture | Learning new systems and new capability.<br>Reluctance to add more complexity, due to fast response times needed.<br>IT security improvements not mirrored in OT. |
| Supply Chains | Increase trust in suppliers & components.<br>Remote access for vendor support.<br>Reliance on supply chain limits current capability.<br>Code of Practice required. |
| Inter-organisational | Collective responsibility across interdependent organisations.<br>Adequate cybersecurity across all market players.<br>Consistent approach.<br>Coordination across stakeholders.<br>Considering risks from an operational perspective as well as a security perspective ensures that cybersecurity risks are managed from an organisational understanding. |
| Evolving Threats | Unknown threats.<br>Preparations for different scenarios.<br>Limited awareness of attack techniques. |
| Incident Response | Consider Availability in real-time environment.<br>Coordination of response.<br>Escalation processes.<br>Accountability.<br>Monitor & detection. |
| Building Capability around vulnerable Legacy equipment | Designing to minimise impact - Assessment of impact and consequences to protect essential functions and processes.<br>Security Updates may not be possible.<br>Vendor support required i.e. agreement to maintain.<br>Security Monitoring to stop attacks more quickly.<br>Identify suspicious access or traffic.<br>Monitor configuration and authentication events.<br>Vulnerability scans to identify legacy systems on network. |

| | |
|---|---|
| | Isolate with network segmentation.<br>Disable unnecessary services and services with known vulnerabilities.<br>Reduce exposure with least privilege access.<br>Change management - Security impact of changes. |

Table 11 Key issues and concerns of DNOs

Advantages were found within as well as between organisations: participation in this work also exposed that different departments in the same organisation had their own approach. The workshop and interviews brought that out, and a plan was made to integrate activities better across the organisation.

An integrated system inherits the security limitations of each interacting component. That's the reality faced in striving to achieve security across organisational boundaries. Transparency of assurance actions is necessary where there is dependency on the cybersecurity maturity level of other actors. Agreement and interworking on cybersecurity requirements within a code of conduct is necessary between generators, DNOs, aggregators and other third-party providers. The communication of this shared energy cybersecurity context provides a step towards that.

The emphasis of this exercise on the needs of DNO organisations was important due to their holding responsibility for the cybersecurity of their operations and services. The compilation of workshop and interview findings later allowed PNDC members to select priority issues that were most important to their organisation which set the focus for future cybersecurity projects at PNDC. While participation was limited to PNDC membership, a subsection of energy sector companies, the outputs hold relevance to the energy sector in general, and beyond the UK, and to the necessity of ensuring an understanding of organisational context for more effective cybersecurity implementations.

## 4.2 ISAC Outcomes

The above findings created the backdrop for the next stage in the research, to exercise improving cybersecurity across interdependent actors within the activities of an ISAC. Cybersecurity was a new consideration in the operational aspect of energy companies, with infrastructure gradually becoming IP connected. The European energy landscape had additional complications due to the electricity grid extending beyond national borders and

being sensitive to cascading effects. This increases interdependencies and the need to work together to secure the system.

The author played a central role in EE-ISAC which enabled this research. Table 12 summarises the activities of EE-ISAC. The outputs of several practice spaces are described in Section 6.1.4. Additionally, the author surveyed experiences of implementing the NIS Directive, among EE-ISAC membership and wider energy sector contacts. Section 6.4.1 summarises the experiences shared, presented as themes that appeared across all responses. With the assistance of ENISA, a sharing forum was arranged between the EE-ISAC and NIS Cooperation Group, including DCMS, to provide anonymised feedback of the NIS survey to national authorities, from a shared energy sector voice. This event marked a first public-private cooperation in energy cybersecurity and inspired the launch of an EU advocacy working group within the ISAC which continues to give a voice to energy sector feedback into regulators and policymakers. The author later created a small practice space to facilitate international cooperation between the US E-ISAC, Japan E-ISAC and EE-ISAC. This developed the relationship into a rhythm of regular sharing on topics of interest. The aspect of 'knowing the group' described in Section 2.1 was given emphasis to meet them where they're at and invite contributions. This intervention assisted in moving from a formal connection between ISACs into active interworking and regular sharing events. These ISAC outcomes are evidence of interorganisational cooperation, including some interworking between technical and policy communities, and beyond the European energy sector.

| Project | Activity |
|---|---|
| **Building a network of trust** | A cultural foundation of the ISAC.<br>Confidential information sharing.<br>Regular slot at member plenary meetings.<br>Sharing experiences on specific topics. |
| **Deep-dive into system requirements** | Investigation of platform use cases.<br>Future system requirements of the ISAC. |
| **MISP instance** | Curating threat intelligence for OT community.<br>Building threat intelligence for energy context. |

| | |
|---|---|
| **Risk management for digitalized energy Systems** | Combine outputs of 3 academic cybersecurity projects on risk management.<br>To inspire practical applications by energy operators. |
| **Threat intelligence** | Combine experience into a living document on threat intelligence management.<br>To share new approaches over time. |
| **Incident response white paper** | A collaboration of members and invited experts.<br>Shared knowledge and experience of incident response tailored to the energy sector. |
| **Public–private cooperation in energy cybersecurity** | A session between the EE-ISAC and the NIS Cooperation Group.<br>Experiences of implementing the NIS directive shared with national authorities. |
| **EU advocacy working group** | A voice for the energy sector.<br>Provides energy-sector-specific feedback, anonymised where necessary, to the regulation and policy arena. |
| **Information sharing with international partners** | Facilitating a regular opportunity for energy-sector sharing with international partners. |

Table 12 EE-ISAC Outcomes

### 4.2.1 Pro-active Incident Response

This research proposes a trusted hub for collaboration across the synchronous grid area. This proposal in Figure *7* offers a synthesis of regulator and operator input during the Network Code drafting process, and is published in the following reference:

Tania Wallis, and Rafał Leszczyna. 2022. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector" Energies 15, no. 6: 2170. doi.org/10.3390/en15062170.

The Network Code is calling for grid entities within the synchronous grid area to establish a SOC capability, either through building their own SOC or via a Managed Security Service Provider. An energy focussed incident response network is proposed in Figure *7* due to the national CSIRT network established by NIS not having a full picture of cross-border risks for the European synchronous energy grid. This is needed to provide the high-level situation awareness that can aid preparations and would support the need for operators to orient themselves to the latest threat picture and build a stronger framework for resilience. A high trust setting is essential for such a network and the EE-ISAC development offers the first steps towards such a trusted hub.

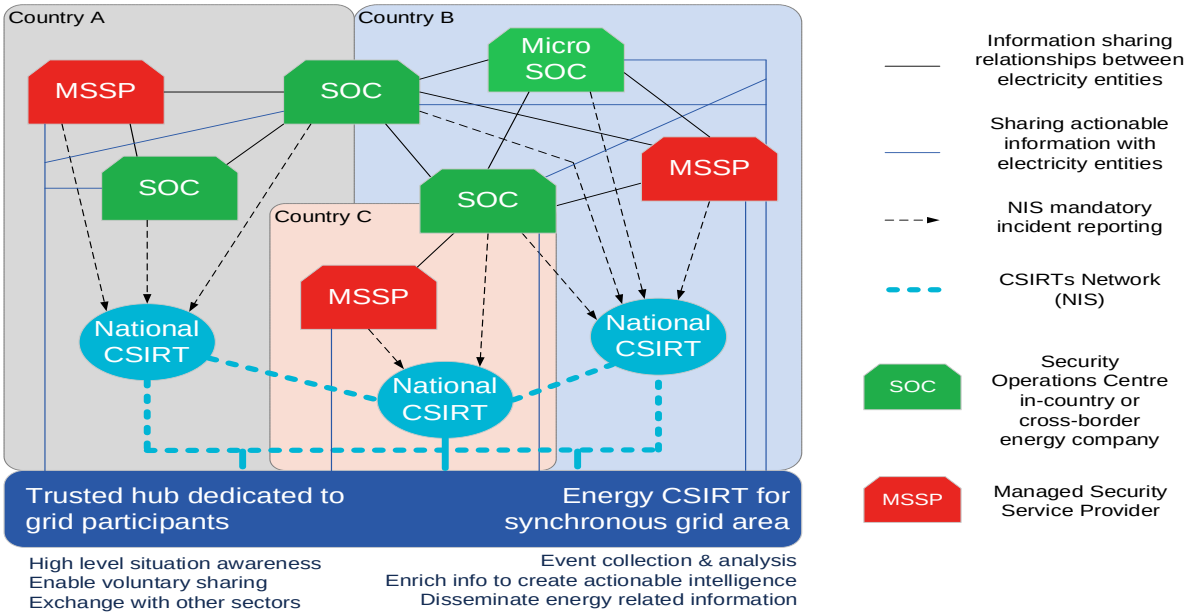


Figure 7 Collective situation awareness and response

### 4.2.2 ISAC Achievements & Recommendations

Table *13* lists the key achievements of EE-ISAC and provides future recommendations. These recommendations are described in detail in Chapter 7 and were formed through analysis of regulatory and energy sector developments, alongside surveying member feedback, and from the author's knowledge of the ISAC. This research proposes the following activities would play an important role in maturing the ISAC:

- 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.

A full analysis of the applicability and utility of EE-ISAC developments is published in:
Tania Wallis, and Rafał Leszczyna. 2022. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector" Energies 15, no. 6: 2170. doi.org/10.3390/en15062170.

| Key Achievements | Future Recommendations |
|---|---|
| Value added for members in cybersecurity cooperation across organisations.<br>Improved understanding of energy sector context for cybersecurity practitioners.<br>Regular events and training. | Innovation is required to leverage the collaboration. |
| Supportive documentation.<br>Testing new research solutions in the energy context.<br>Platform improvements, investigating utility of supporting tools. | Regular evaluations of efficiency.<br>Development of threat analysis centre capability. |
| Energy operators at the core of activities have assisted useability and acceptance.<br>Acts as a voice for the energy sector, provides feedback to policy arena. | Extension of situation awareness.<br>Providing more actionable threat intelligence. |

Table 13 EE-ISAC Achievements and Recommendations

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 threat 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.

## 4.3 Supply Chain challenges identified

The research and analysis of NIS implementations, from the perspectives of the different roles involved, resulted in the following findings and recommendations. These were presented to the UK Cabinet Office & Lead Government departments and are published in:
Tania Wallis, Chris Johnson, and Mohamed Khamis. "Interorganizational cooperation in supply chain cybersecurity: a cross-industry study of the effectiveness of the UK implementation of the NIS Directive." Information and Security: An International Journal 48, no. 1 (2021): 36-68. doi.org/10.11610/isij.4812.

- **Responsibility -** Holding responsibility for operational impact and consequences on a physical system makes it harder to divide up responsibility and transfer risk between parties.
- **Commercial vs technical arrangements -** High level expectations are encapsulated in contractual arrangements with suppliers but the level of detail is insufficient for deployment at a technical level. Previous research suggests that a mutual commitment to cybersecurity through trusted partnership has the potential to achieve more than formal agreements [58].
- **Balancing control with cooperation -** A balance of regulatory and contractual controls with support for the necessary collaborations is required to drive improvements [58].
- **Top-down & Bottom-up -** There is a place for generic frameworks to guide the sector and drive improvements, however there are specifics to be worked out between customers and suppliers, to translate risks to component level and engage suppliers appropriately.
- **Integrated Processes & Skillsets -** Rather than achieving an effective division of responsibility, there is more likely a need for integration of processes. Access control, vulnerability management, incident response are all areas where there is overlapping activity between customers and suppliers, and a need to integrate their processes. Indeed, a collaborative commitment to solving problems together is the reality, with skillsets coming from customers and suppliers, IT and OT, bringing an understanding of operational context together with supplier knowledge of products being deployed. Engaging suppliers in reducing the impact of incidents through joint exercising.
- **Points of Governance with the Supply Chain –** It is necessary to examine touchpoints with the supply chain from procurement through the life of a product or service to identify where there is effective transfer of risk or knowledge or a mutual commitment to cybersecurity with proactive and useful information flows between partners.

### 4.3.1 Supply Chain Research Outcomes

More clarity in oversight is needed to go beyond addressing individual companies' business risks and achieve the required level of cybersecurity for national infrastructure. The author's proposed assurance framework is published in the following reference, and was presented to the International Conference on Cyber Situational Awareness, Data Analytics and Assessment in 2020:

Tania Wallis, and Chris Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-10, doi:10.1109/CyberSA49311.2020.9139641

The guidance coming from NCSC outlines four key stages to supply chain security [59]:

1. Understand the risks
2. Establish control
3. Check your arrangements
4. Continuous improvement.

The supply chain oversight aspect of the NIS Directive requires a substantial effort by OES to assume responsibility for the cybersecurity of supply chain tiers. The first stage of 'Understand the Risks' essentially should expand into managing those risks. Establishing an achievable level of control involves defining and agreeing supply chain involvement in the cybersecurity process of protection, detection, response and recovery. Checking agreements and contractual arrangements requires a regular assessment of suppliers' contributions to cybersecurity capability. Achieving a cycle of continuous improvement would be aided by managing dependencies on suppliers to achieve the required improvements. Figure 8 demonstrates some of the activities required in each of these four stages and indicates that continuous checking of supply chain arrangements will require a performance monitoring activity in order to identify interventions and improvements where most needed. Section 9.6 outlines some future work in this area to propose supply chain metrics to monitor improvements and identify gaps in coverage.

The information gathering activity in 'Understand the risks' must be ongoing and linked to 'Continuous Improvement' hence it has been described here as a Governance activity that includes agreeing accountability and assigning ownership of the risks.

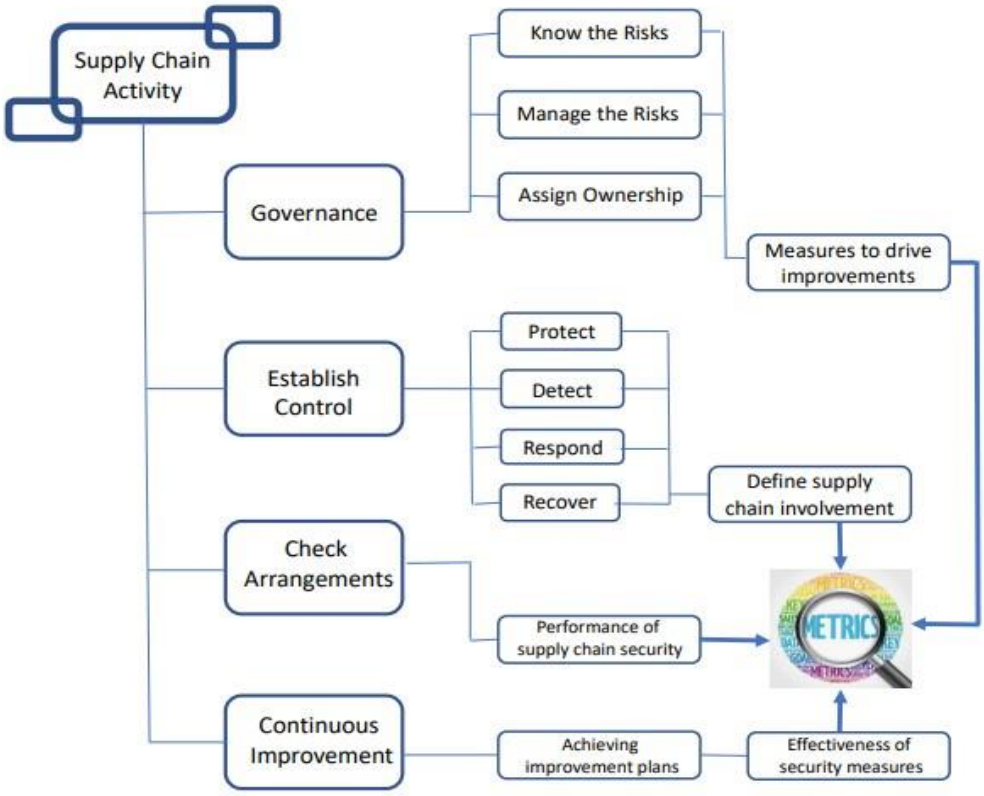


*Figure 8 Supply Chain Activity*

The chart in Figure 9 expands further this Governance activity. In order to 'Know the Risks' OES are including cyber security assessments in their procurement processes to understand the risks presented by each new supplier. This is enabling a level of importance to an OES's essential service to be assigned to each supplier and a corresponding response in terms of assuring a suppliers' compliance with security requirements. The level of oversight of suppliers is prioritised according to their involvement in providing and supporting critical assets and services within the scope of NIS. Achieving this with existing suppliers as contracts are renewed to include cybersecurity requirements is a more gradual, long term process.

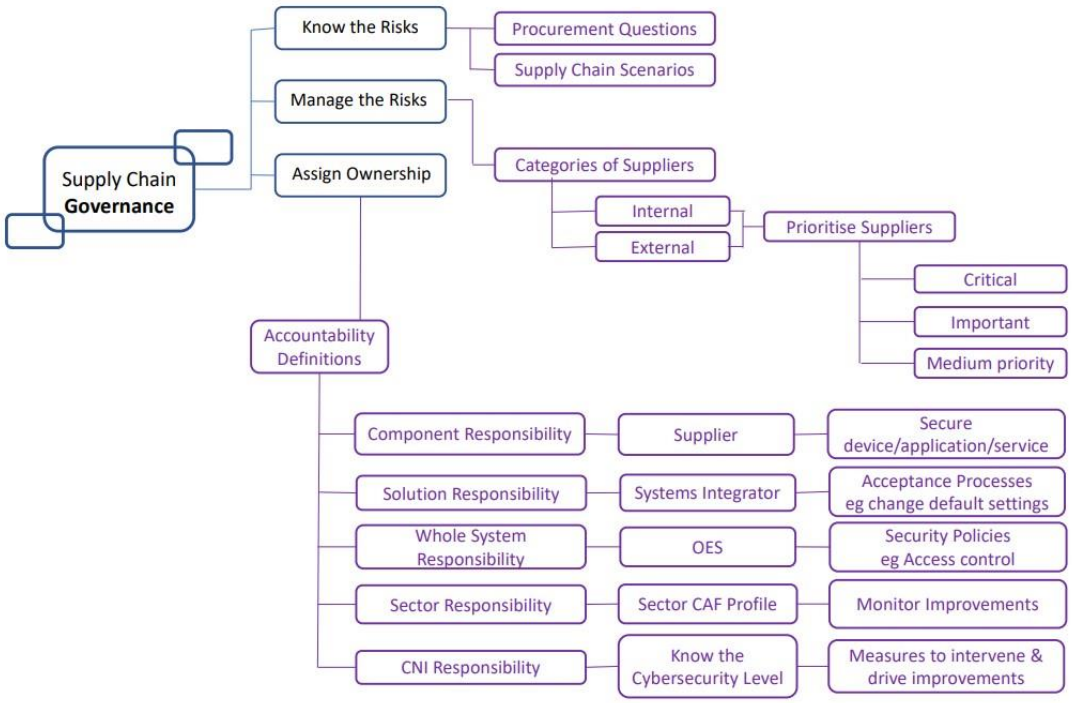


*Figure 9 Supply Chain Governance activity*

The return of procurement questionnaires by amenable suppliers is providing a partial picture but is a long way off the more complete visibility required to really 'Know the Risks'. Individual security questionnaires coming from each customer are causing a considerable overhead for suppliers. With a fair proportion of this activity covering common ground, this points to potential for developing common methods and improving efficiencies in security assurance. For a more effective accountability, roles and responsibilities and achievable goals need to be clearly articulated with a consensus on the value of the defined approach [60]. The value-add in procurement processes could be improved upon through better analysis of responses to the question set and sufficient follow up to ensure requirements are met.

Guidance on potential attack scenarios to prepare for would also assist in focusing activity towards evolving threats. The NIS Directive expects OES to know and understand their risks and the threats to their sector. However, the uncertainty in this area has been consistent. This is where government can offer a meaningful contribution through assisting OES to form a clearer threat picture [61].

The NIS Directive has been formulated in a way that assumes OES to have a hierarchical control over their supply chains and the CAF expects a deep understanding of the supply chain [62]. The process of implementing NIS is presenting areas of their supply chains where OES have less negotiating power, or a lack of choice in suppliers, to influence the required level of cybersecurity. Tiers of the supply chain are not managed or understood. A very limited visibility of sub-contractors is common. Longstanding contracts often do not include cybersecurity requirements and legacy equipment lacks the capability to provide security.

Oversight by CAs is looking for shared responsibility models to be agreed with suppliers [62]. The standard IEC62443 on security for industrial automation and control systems is made up of component, system, policies and overview levels [63]. Responsibility for the security at each of those levels needs to be assigned appropriately, as suggested by the accountability definitions in Figure 9.

Self organising networks have developed to work together on these issues. One sector has taken this approach through a committee of several OES meeting with critical suppliers one by one to discuss their common security requirements. This can succeed as far as the significance of their shared common denominator. This OES network would also prefer to be able to meet with suppliers as a group to develop some consistency and new norms with their key security requirements. There is potential for governments to do more with coordinating and motivating these self-regulating networks [61]. The current ad hoc approach, while all the risk in the supply chain is held by the buyer, needs a clear mechanism to be developed that can accommodate the dynamic property of this situation such that changes or new vulnerabilities in the supply chain, that are likely to impact with high consequences, can be flagged appropriately.

While the NIS Directive is being adopted by individual OES to varying degrees, the actual contributors to their overall cybersecurity level comes from a broader set of organisations. Systems integrators are not always receiving appropriate direction or guidance in terms of clearly defined acceptance processes or end to end system security requirements. Beyond knowing the risks and the current cyber security capability is an ongoing activity that requires governance and oversight to manage the:

- Contributions to reducing the attack surface.
- Contributions to understanding the latest threat landscape.
- Contributions to minimising the impact of incidents.

Otherwise decisions will continue to be made in isolation or without reference to clear security requirements or a full risk picture.

## 4.4 Overall Summary of Research Outcomes

Table 14 lists the full set of outcomes from this thesis.

| Practice Space | Who was involved? | Action | How was this done? | Outcomes |
|---|---|---|---|---|
| PNDC Workshop | Energy companies, Telecom service providers, Suppliers of automation & smart grid equipment. Consultants in Security & Risk | Whole group activities. | Presenting perspectives on the problem. Sharing breakout discussions with wider group. Categorising outputs together. Highlighting common and important issues. | Views on issues and challenges captured. |
| PNDC Workshop | Facilitators & participants | Breakout groups | Questions and dialogue. Brainstorming issues. Observations. | Record of interaction in each group. Debrief with whole group and with facilitators. |
| PNDC Workshop | Facilitators | Post-workshop debrief. | Analysis of notes and discussion to clarify workshop outcomes. | Learning from workshop informing follow up interviews. |

| | | | | |
|---|---|---|---|---|
| PNDC Membership | Author | Interviews with DNOs. | Semi-structured interviews including open discussion. | Further information gathered on issues and challenges for each PNDC member. |
| EE-ISAC Membership | Author | Creation of practice spaces on relevant topics. | Discussion, visioning, planning with Members. | Proposed work items agreed with members and Board. |
| EE-ISAC Synthesis of knowledge | Academia & Energy operators | Synthesis of risk research outputs, into a useable form for utilities. | Presentations of risk management projects, highlighting relevant learning points for utilities. | White paper on risk co-produced by academia and energy operators. |
| EE-ISAC Synthesis of knowledge | IT & OT experts, academia, energy operators. | Incident response tailored to energy OT context. | Workshop and dialogue to synthesise experiences. | White paper on incident response. |
| EE-ISAC | European energy operators | NIS Implementation | Survey of experiences. | Feedback to policymakers. |
| EE-ISAC | EE-ISAC members | Review of ISAC progress. | Live Questionnaire. Open dialogue while answering questions, voting with post-its. | Member views on progress and next steps. |
| European Energy Sector | Author | Proposal for enhanced cooperation in cybersecurity. | Observation of Network Code developments, NIS evolution, dialogue with energy actors. | Trusted Hub for grid participants, and recommendations for ISAC maturity. |

| | | | | |
|---|---|---|---|---|
| Supply Chain | Operators Suppliers Competent Authorities | Research the Supply Chain aspects of NIS Implementation. | Semi-structured interviews. | Challenges with securing supply chains. |
| Supply Chain | Author | Enhancements to supply chain cybersecurity guidance. | Synthesis of interview findings with existing guidance and supply chain management literature. | Governance structures for supply chain cybersecurity. |
| Supply Chain Expert Group | Operators, Suppliers, Systems Integrators, Manufacturers, Consultants, Academia | Review touchpoints with supply chains and assess need for partnership approach. | Presentations of perspectives. Dialogue. Identify challenges and gaps. | Future Work plan for co-production of supply chain OT guidance. |

Table 14 Summary of Research Outcomes

## 4.5 Limitations

- The knowledge from this research is mainly situated with DNO members of PNDC and DSO members of EE-ISAC, due to the research activities mostly being restricted to participants from the PNDC/ISAC memberships. However, the PNDC/ISAC membership represent a fair cross section of the UK and EU energy sector, and wherever possible different expertise was invited to cover gaps and assist the process.
- The supply chain aspect of the research depended on building new contacts in new sectors. While there was interest to engage due to the research area being of significant concern to many practitioners, the supplier interviews were limited to larger suppliers to ICS with more mature cybersecurity. Future work is considering uptake by smaller businesses.
- The practice groups combined a diversity of skills and expertise but were quite small groups, but this helped the close synthesis and outputs were provided for wider review.

- The solution-oriented approach, that was aiming for cybersecurity improvements for critical infrastructure, meant the interdisciplinary and trans-professional experience, or cross-sector immersion into broader perspectives, was not reviewed interpersonally with the participants. The solution-oriented focus was respected as the nature of striving for a safe and effective engineering solution. The research outputs are therefore presented in terms of ability to co-produce effective and useful outputs from the interaction of knowledge.
- The practice group involving the PNDC community had a bias towards exploring projects suitable for the PNDC facility so the direction of the responses was influenced by not only the skills and interests present but also the interest to explore where additional support from PNDC research may be needed. However, this assisted the uncovering of what could be dealt with in-house by the industry participants and where partnerships could be required to meet cybersecurity challenges.
- The potential increase in cybersecurity maturity levels or capability improvements for single organisations, as a result of their participation in the practice spaces, has not been analysed directly. However, willingness to contribute to these groups naturally implies some individual benefits from participation, and appreciation for the cross-fertilisation of knowledge was expressed by several participants.

## 4.6 Overcoming Challenges

- Ownership of the problem – this work looks at issues that are between and beyond individual organisations. It required the interest and ability to look beyond individual business viability to a more holistic view of CNI and encourage that in others through communicating the vision of the work.
- Discrediting academic process/outputs, participants wanting solutions to problems more quickly, being less interested in academic details. The emphasis on co-production of outputs in the practice groups helped to overcome this and integrate the activities and interests of academic and non-academic actors.
- For the work to go beyond just bringing various actors to the table, designing new and robust pathways forward required individuals or companies to be interested and to benefit from their participation. Instead of being users or beneficiaries to

academic output, others were being more actively involved, with practice groups including academic/industry/government actors. Involvement in the work had the potential to assist participants in their own role and professional development.

- Overcoming biases – The author's ability to sit between disciplines rather than coming from one area of expertise was beneficial to provide less bias in shaping the work. This was aided by combining and including a wide set of perspectives, and the use of reflection and continuous learning. Introductions from each member helped to make sure their interests, assumptions and requirements were known to all participants early in the practice groups. It is also recognised that being a participant observer, in a central role, can introduce bias in itself. However, a full immersion into the interorganisational experience was also an essential component of the research.
- Expecting voluntary effort from participants to work beyond their own organisation was encouraged by a shared interest and common needs, however participants also needed to gain individual value to be motivated to put in the effort required. The common mission of cyber professionals spurs them to donate effort to endeavours such as the practice groups in this research. The nature of cybersecurity being beyond the feat of a single organisation encourages a loyalty to wider networks. However, in most cases participants require support from their organisations to give resource to the activities.

Having some governance and facilitation capability at the centre of the practice groups, to hold the vision, guide the process, and bring together diverse threads, is essential to produce significant outcomes together. Support from government, academia or industry associations is necessary to provide such capability. Without responsibilities assigned for co-defining common requirements, or acting together on shared issues across organisations, this can lead to a lack of synchronisation in complex systems, and asymmetries across supply chains. Standards and guidance, proven approaches, and illustrative examples, contribute in part to resolving these issues. However, there needs to be equal attention given to reorienting, to adapt and reposition, through regular evaluations of continuously evolving environments.

# 5 Securing the Operational Context of Energy

This chapter sets the scene for energy cybersecurity by investigating future energy scenarios and researching the realities of securing an operational environment.

The content of Chapter 4 has been published at the following reference, and was presented to the Energy Networks Association and at ESORICS 2021 Workshop.
Tania Wallis, Greig Paul, and James Irvine, "Organisational Contexts of Energy Cybersecurity," Conference Proceedings SPOSE2021 at ESORICS. Lecture Notes in Computer Science, vol 13106. Springer. https://doi.org/10.1007/978-3-030-95484-0_22

The energy system is going through huge transformation to integrate distributed renewable generation and to achieve the goals of net-zero carbon emissions. This involves a significant adjustment to how the system is controlled and managed, with increasing digitalisation of technology and growing complexities across interconnected systems. Traditionally electricity networks adjusted their supply of energy in response to changes in demand. The future energy system will require more flexible demand to be able to use or store energy when renewables are generating. This change is exacerbated by additional demand for electricity for heat and transport uses.

Utility organisations hold responsibility for securing their networks and assuring the supply of electricity. This section describes a full investigation of cybersecurity issues and concerns for utilities. This industry review was carried out to provide a thorough organisational context for the ongoing design of cybersecurity improvements in the energy sector. The assessment of potential impact and consequences of cyber-attack is recommended in Section 5.2.8 to direct necessary preparations towards protecting essential functions and processes. Improving resilience across interdependent actors is discussed and resilience measures suggested in Section 5.4 to guide the contributions of different actors towards whole system resilience.

Energy distribution networks are undergoing significant change. Traditionally based on a relatively smaller number of central generation sites with simple control and stability through overprovisioning, generation is becoming increasingly distributed with the introduction of renewables such as solar and wind, the network is becoming a 'smart grid'

with enhanced control and demand management to improve efficiencies and reduce overprovisioning, and the net zero agenda is increasing demand on the electricity network through the electrification of heat and transport. This has significant cyber security implications. Electrical distribution networks will have to interact more with sources of supply and demand, and more sophisticated control is more vulnerable to attack.

## 5.1 Preparing for Future Energy Scenarios

With uncertainties about the impact of cyber security on organisations within the energy sector, exploring potential scenarios can help direct more effective preparations. Each scenario gives us a future vantage point from which to observe the present situation. The capacity to manage future uncertainties requires both learning from past attacks as well as consideration of different futures [64].

### 5.1.1 Setting the Context

National Grid operates the transmission network in much of the UK. Its future energy scenarios (FES), shown in Figure 10, offer a context to explore potential cyber security scenarios and impacts. Four different pathways are described towards net-zero carbon emissions, including consumer or system transformation as different ways to reach 2050 goals [65]. The FES will require an integrated whole system approach to manage a more complex picture of power flows and to coordinate demand with supply.

Stronger and faster interactions are expected between different aspects of the energy sector, to obtain value from coordinating and optimising the whole system. The wide adoption of data-driven insights to manage a distributed energy system must be balanced with the necessary attention to cybersecurity and privacy. From a policy perspective, attention is being paid to securing consumer smart devices in the FES, both in terms of the devices themselves, and their interactions and data flows required. In addition to privacy concerns, where different actors and devices have control and can trigger changes to the system, a coordinated and secured approach within safe parameters must prevent unwanted consequences.

Electricity markets driving consumer demand with price incentives will necessitate digital solutions to prevent sudden swings in demand. For example, Electric Vehicle (EV) charging

patterns will need to be managed to spread the load away from peak demand and towards periods of higher renewable generation.

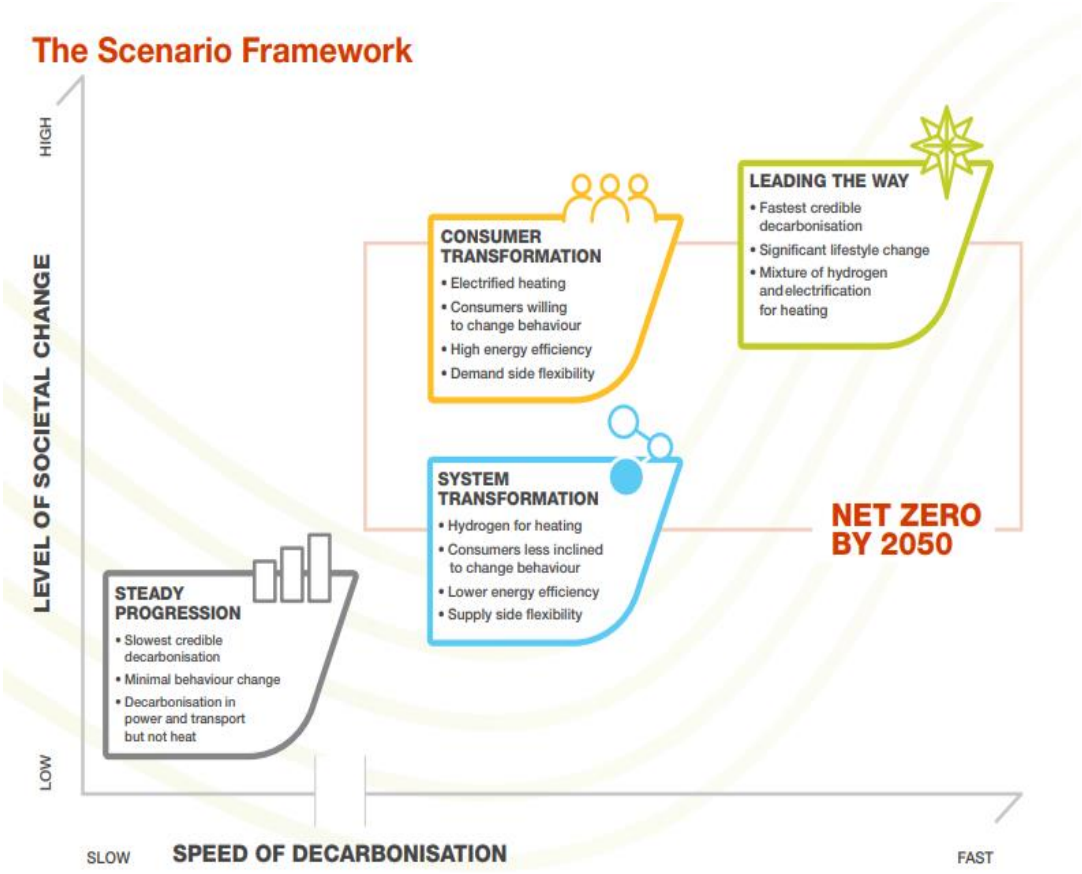


*Figure 10 National Grid Future Energy Scenarios* [65]

While these future scenarios point to an increasing need for digital solutions, a consequence driven approach to cybersecurity is emerging through cyber informed engineering that recommends keeping reliance on digital technology to a minimum for critical functions and processes [57]. [36] It will be important to prioritise essential functions by protecting the hardware, software, processes and procedures that enable them, in order to prevent unwanted consequences [66]. Analysis of these new scenarios with new dependencies will identify potential impacts to avoid, where it is most necessary to reduce pathways for malicious control of essential assets and functions. Particular attention will need to be given to reliance on offshore wind, aggregation of flexibility services, energy storage and the capability to spread new load patterns towards renewable generation patterns. Network reinforcements will be required for distribution networks to cope with

increasing power flows, especially to meet electrification of heat and transport, and to avoid the constraint of renewable generation. The cost of this "can be minimised by deploying smart and innovative non-build solutions" and through better integrated planning [65]. Traditionally the energy system had supply responding to changes in demand, the new scenarios put supply in charge and expect smart flexible demand to either use or store electricity when it is available. To prevent opening additional pathways to attack, cybersecurity must be embedded into these smart solutions.

All these FES will need the support of a highly interconnected control structure, and will also increasingly interact with natural gas, hydrogen and biofuels. Aggregated technologies on the demand side, responding to half hourly price signals, will require managing at street, local and regional level so that distribution network to protect system stability. A whole street of EVs responding to price signals, all drawing or all feeding back power to the system, could otherwise cause instability. The report[67] expects a "deep digitalisation of all energy assets". This will require secure solutions at all levels. "As new sources of flexibility come online, we will need their operational data" [67]. Information becoming available in more places could also be assisting adversaries to build a clearer view of the system. The transformed energy system will require "interaction between digital platforms, technologies and markets signals" and "interoperability across data, services and technologies" [67]. An increasingly interactive and interoperable energy system must be developed with cybersecurity in mind.

With this opening up of access to data and lots of pathways into networks, it is likely to become too much to monitor for anomalies without some simplification to effectively oversee the cybersecurity of such solutions. The integrity of data is essential where it is being used to control devices and system responses. An honest look at our reliance on complex digital solutions, and the recognition that we will have "combined technologies, delivering multiple services", "smart technologies, all digitally enabled" and "deployed at scale and throughout the energy system" [67] makes it clear that cybersecurity must be fully embedded into the journey to net zero. Where dependencies are greatest and to protect essential functionality, priority decisions will need to be made. An engineering perspective must find ways of defending an extensive attack surface such as keeping system capabilities within safe limits, while retaining the system orchestration that digitalisation brings.

## 5.2 Researching the Industry Context

A thorough research of organisational context was carried out before looking at specific areas where solutions were needed. This was to discover the main points of concern around the cybersecurity of utility networks and to communicate the context that future solutions needed to function within. The process provided useful learning for the practice group. Participants were getting to know new capability and new systems, that would form the future energy networks. There was a need to construct a picture of the situation and re-create mental models that more closely match the environment. Developing this shared understanding provided a foundation for more applicable cybersecurity solutions.

This work commenced with a cybersecurity workshop attended by various energy sector actors, connected with the PNDC, including Distribution Network Operators (DNOs), vendors and consultants. Follow-up meetings and discussions were then held with participants to build a full picture of the situation. This provided a thorough organisational context for ongoing design of cybersecurity improvements and to prioritise innovation projects at PNDC. The methodology used and spread of participants was described in Section 2.4 and the key findings were previously summarised in Section 4.1. The following sub-sections describe the emerging cyber security issues and requirements for these energy sector organisations. There was a bias in the practice group towards exploring projects suitable for the PNDC facility so the direction of the responses was influenced by the skills and interests present and the need to explore where additional support from PNDC research may be needed.

### 5.2.1 Accessing multiple sites

There is a requirement for security of both local access to equipment within a substation's own network and remote access to substations over wide area networks. The need for remote access support for substations is required from third parties, vendors and external contractors. Corporate network access into substations was also felt to be essential, requiring an economical solution which meets the needs of different branches of the business, yet preserves security of the operational network.

There was a strong requirement for Identity and Access Management (IAM) capability, with a need for logging of actions, as well as control of who is able to access systems, and a facility

for revocation of access, while considering the unique nature of an operational network and ensuring availability of systems. To avoid the introduction of complex security systems which slow down operations, operational networks often do not feature the same security features as corporate networks, such as 2-factor authentication. Introducing stronger verification of the identity of a party connecting to equipment, as well as the actions they are permitted to carry out, must consider the operational context of an always-on environment.

In a control room setting, it is difficult to switch the identity of the operator without shutting down and restarting the interface which is not appropriate for a real time environment. There are layers needed to the solution, and there is a different class of problem for unattended equipment.

For remote access there were issues with creating VPN tunnels into substations such that alternatives to VPN may need to be considered. A specific concern was how to manage cryptographic keys and VPN configurations, and in making coordination and management scale to the high number of substations sites.

There were different views on the extent of encryption and whether it is necessary for all communications to be encrypted or would authentication alone offer sufficient security for certain services. Grid protection applications, in particular, could require very fast, potentially sub-millisecond encryption to meet latency requirements.

There was a desire to look into “encrypted by default” communications within operational networks, provided suitable provisions are made for availability, reliability and performance. However, there was a concern with regard to the security and management of certificates and cryptographic keys, and ensuring the correct handling of issuance and revocation, to avoid any downtime or loss of functionality.

Specific technologies for linking sites were discussed, such as whether there were any security benefits to using MPLS over more traditional technologies. There was considerable concern about the widening cybersecurity issues caused by moving towards IP-based networks and IEC 61850 substations.

There are some unique challenges within operational networks which can make deployment of standard solutions more complex, such as most single-sign-on systems failing if the

centralised authentication server fails or goes offline. It would be possible to build a more resilient solution using Public Key Infrastructure (PKI) technology, to securely authenticate parties through certificates issued on a regular basis, with no direct requirement for the authentication servers to remain online to permit remote access to systems during outages or other emergency scenarios. For log aggregation, the main priority would be ensuring provenance of the logs against tampering, while keeping bandwidth usage to a minimum for remote sites which have limited network link capacity available for log aggregation. PKI was seen as a potential approach to securing networks, although the risks of quantum computing advances were highlighted as DNOs – and regulators – traditionally expect relatively long-term deployments of equipment.

### 5.2.2 Securing Legacy Equipment and Future Networks

There is a significant challenge in managing legacy equipment as the network moves to a more integrated environment with inter-connected systems, especially as legacy equipment was often not designed with this in mind. Legacy devices frequently lack access control and other security measures, and assume the network is only available to fully trusted devices. It is not possible to change, modify or update legacy equipment to be compliant with newer security systems, and many older security protocols feature weaknesses which cannot be resolved other than by updating to a newer version of the protocol such as Transport Layer Security (TLS) protocol.

If legacy equipment has no access control, any party with access to the network to which that device is connected may interact with the equipment, and potentially carry out operations. To maintain the security of such devices, it is necessary to firstly identify these devices, and secondly ensure that they are isolated from other network traffic with network segmentation, and from remote users with VPN access, limiting access to nodes that specifically require it. Legacy equipment almost invariably has no logging or auditing capabilities, meaning that attempts to gain access to the equipment may not be detected. Building adequate secure capability around legacy systems is essential. Security monitoring is vital to stop attacks more quickly, identify suspicious access or traffic, and monitor configuration and authentication events.

Lifetime management of equipment is an issue, including ensuring suitable vendor support, particularly for embedded systems where security updates are not necessarily forthcoming a small number of years after release.

The practical security considerations of firmware updates on equipment in the field were also raised. There is a perceived risk of updating working equipment, due to the loss of availability while updating or other failure due to the update. However, software vulnerabilities present a serious risk to the security of the network, and insecure devices could be used as “pivot” points to explore other parts of the network, potentially exposing more critical systems to attackers. The risks of allowing non-updated devices to remain on the network needs to be evaluated, perhaps using penetration testing outcomes, versus the risks of carrying out an update (ideally remotely), and the impact on security and availability this may have. Another risk introduced through remote updates is the potential for an attacker to use this method to deploy a malicious update, indicating a requirement for remotely updateable devices to have suitable security in place to authenticate any updates issued.

With a large number of embedded systems deployed in the network, an interest was expressed in whitelisting technology, which could be used to constrain embedded devices to mitigate against malicious software or other attacks, by ensuring that only the specific software originally installed on the device would be able to execute.
To improve the integrity of the OT environment, there could be potential for the use of VPN tagging to monitor data flows and record log in access and operations on legacy equipment which may not currently have support for this.

### 5.2.3 Network Monitoring

The introduction of malicious equipment to a secure network is a security concern. Having the capability to monitor networks for the introduction of new devices, or changes to existing devices, would reduce cost and provide a more rapid response. Additionally, identification of specific unusual traffic is a potentially beneficial proactive measure, in order to attempt to gain early warning of unusual behaviour on a network, or of a device being compromised. The benefits of monitoring also extends to monitoring devices for important security updates, to ensure that each device is patched against any known vulnerabilities, and

running the latest approved software revision. This process could be combined with targeted penetration testing to identify widely deployed devices which should be tested to ensure no obvious vulnerabilities are present. However, controlling and verifying devices present on networks is challenging given the numbers of devices involved.

There was a need to improve visibility of all devices connected to networks. Most large systems such as servers had agents installed, but no monitoring or control of the devices present, or how they are managed and patched.

The need to better understand the traffic experienced within SCADA networks was recognised. Concern was raised over how to correctly identify both “good” and “bad” traffic within a network, for intrusion detection and prevention systems. There were questions over when to stop traffic, and risk interrupting availability, versus permitting and then investigating after-the-fact, since detections systems are generally preferred for SCADA environments.

There was an interest in log aggregation for auditing and accountability of actions, which was felt to be a growing concern in the future with increasing remote access. There are challenges with limited bandwidth to some remote sites, and a need to ensure logs are transmitted securely.

The transition to IP-based networks brings about opportunities to improve resilience and availability by removing reliance upon centralised points of failure. Such a change would lead to significant alterations to network design and organisation, specifically around security. A distributed trust management approach would permit equipment to communicate only with other authorised devices, ensuring that any unauthorised devices introduced to networks would be unable to interfere with or communicate with authorised devices. Such an approach, without requiring a single centralised point of failure for authentication, was identified as a potential area for future work, particularly applying the concept of distributed trust in a non-product specific context.

### 5.2.4 Building Incident Response Capability

Capabilities to identify, respond and recover from a cyber-attack are limited at present. The current power system was not designed to handle the effects of a cyber-attack. It has been

designed with n-1 redundancy as a goal, to handle the loss of generation or transmission assets. In the context of cyber security, there are many other scenarios to be prepared for. There is a need to develop faster detection of malicious or unpredicted activity and to design appropriate responses to potential cyber incidents.

Appreciating the differing context of an OT environment is crucial to handle cybersecurity in an appropriate way for an operational setting. The focus leans towards protecting systems and restoring operations. Incident responses must consider real-time and availability requirements. For example, control systems cannot be disconnected from the network if under attack like an office computer could be. Cyber-security responses appropriate for an OT environment are needed.

**Defining Responsibility.** Part of incident response will be to define the level of incident handling within an operator's capability and agree responsibilities within and across organisations. Operators need to decide what needs to be passed up to, for example, the National Cyber Security Centre (NCSC), or how to engage a response across supply chain organisations, so that an incident response structure can be agreed. Also, identifying where practical help may be needed to withstand an attack, especially over a long time period: e.g. a sustained Denial of Service attack for several days. An effective coordination of the response needs to also be established so that crisis management procedures are in place for cyber security. Previous cyber-attacks have highlighted the use of cascaded attacks to reduce the efficacy of responses. Crisis management must also consider how procedures would be implemented under degraded communications, or following the failure of communications infrastructure as a result of the attack.

To resolve attack situations, organisations will need to build a reliable and strong network of partners for incident response and recovery, as well as agreeing on escalation processes and responsibility levels within and between organisations.

### 5.2.5 Knowledge of threats

With an uncertain picture of evolving threats, utilities are expected to prepare for unknown threats to their essential services. Concerns were raised over being without a formal threat landscape for operational networks. While the latest threat landscape is constantly evolving, intelligence gathering could indicate attack trends and future security risks and help to

prepare for new scenarios. The potential for an interactive platform to share an evolving picture of threats was discussed. While there are clearly some challenges to producing an all-encompassing threat landscape model, it was felt that most work is being carried out "in the dark", with limited awareness of the types of attack techniques that could be faced.

Identifying various scenarios will aid the preparation of responses to cyber incidents. It is important to consider how vulnerabilities in digital components could cause failures across the grid and to consider different threat agents and types of attack. This will help to identify high impact scenarios and build up a picture of the potential scenarios that need to be prepared for to reduce the impact of attacks.

### 5.2.6 Electricity sector specifics

There is the risk of single site compromises cascading into a wider system threat and affecting other organisations as well. It was noted that the involvement of cross-DNO working groups, such as NCSC or Energy Networks Association (ENA), would be needed in these circumstances. Being unprepared for cyber incidents exposes the system to the risk of cascading effects which could result in a brownout or even blackout situation. There is also the risk of manipulation of or loss of control and monitoring systems. The ability for an attacker to exert control over large loads, or indeed a significant number of smaller loads, could adversely affect system balancing and lead to blackouts. Likewise, malicious control of generation could affect supply and cause instability.

**Real Time Performance**. There are technical challenges with securing protection communications, due to the need for ~4ms response times, and the perception that this is difficult to achieve alongside secure communications. A cost/benefit and performance analysis was felt to be necessary for securing extensive distribution networks. The security risks to assets from secondary substation and below needs further investigation. The impact of encryption on performance and availability to discover where high speed encryption applications may be needed. Encryption, for example, could add cost, without providing sufficient benefit.

**Active Network Management.** The introduction of connections to third party generation stations, outside of DNO security controls, policies and visibility is adding a new dimension to their threat scenario. New technology such as Active Network Management (ANM) is

presenting DNOs with new security challenges. ANM requires connections to both the primary control network and secondary telemetry networks, limiting the traditional approach of segregating these networks. With the potential introduction of servers and other equipment within substations, and wider deployment of connected monitoring equipment, itself vulnerable to attack and manipulation, a more ANM-oriented network is going to introduce new security and management requirements. This was considered important, due to the ability for ANM to interact with and control generation equipment on third party sites and networks.

Each 3rd party is different so a standard connection agreement would simplify things and being able to monitor and identify unusual activity over remote connections for further investigation. While the priority is to make DNO systems robust first, before trying to deal with imposing security requirements on the third parties and generation operators, but the risk needs to be more shared.

This work was presented to The Energy Networks Association (ENA) who later formed a working group to create the connection guidelines for Distributed Energy Resources (DER) to facilitate meeting cybersecurity requirements with small generators. They now require consultation and collaboration between the DER operator, the distribution network operator and any third-party providers involved [68]. Similar agreements attending to cybersecurity will need to be developed for the coordination and connection of increasing amounts of offshore wind generation.

### 5.2.7 Organisational culture

Unwillingness to risk introduction of complexity which may otherwise impact on availability means that operational networks frequently lack the same security measures found on corporate networks, such as 2-factor authentication and other measures to ensure security during sign-in processes.

The challenge of management not being familiar with the currently deployed systems was also highlighted as a concern, given the significant changes in approach to security required with newer, more interconnected equipment. Another challenge identified was in keeping up with advances in IT, and security in general. The pace of change and developments, and the speed with which information about vulnerabilities may be disseminated makes it

difficult for small cyber security teams to keep up to date with information. A need for training in cyber security was also highlighted, to ensure everyone who needs it has a strong basic knowledge of the essentials for securing systems. The ability for a 'small' mistake to completely compromise the security of an installation was a concern. An example given was of an engineer bridging the 'secure' operational side of the network to a WAN link using a patch cable while working on equipment. Knowing the organisational context that security solutions are to be implemented and maintained within gives a broader view of what is needed to build a security culture and more secure ways of working.

Overall governance of cybersecurity within the organisation as a whole needed some attention. Progress had been made in different business units but had resulted in different approaches and security policies, which would be better unified and coordinated. There was interest in establishing a broad governance and security architecture, to create an ideal state to aim towards when deploying and designing systems.

**IT/OT Integration**. The organisational boundaries between operational and corporate sides of IT provisions were also highlighted as being a concern – equipment not installed by IT and not connected to the corporate IT network was considered to be outside the responsibility of IT. Advances in corporate security (single sign-on, enforced 2-factor authentication etc.) have not been replicated on the operational network due to IT not having visibility of activity on the OT side.

It was recognised a new model for working was required to manage the increasing numbers of computer systems (such as servers) in operational networks. There was a desire for the IT teams to manage such systems, as this was more within their area of expertise, but this presented challenges such as providing access for corporate IT staff into substations. Specialist OT engineers may not be available 24/7 to assist during incident response leaving IT to deal with issues but with limited understanding of an OT environment. Also, IT approach to changing settings and parameters may not align with OT change control procedures.

**Supply Chain Security**. Based upon the significance with which it was emphasised by all DNO members consulted, some of the largest risks to DNO operations appear to be posed by their supply chains, and by connections which are permitted from external third parties, operating

outside the control of the DNO's business and security policies. Taking some measures to begin to increase the level of trust in suppliers and components is an important step.

Equipment vendors increasingly wish to have remote access abilities to provide support. This introduces risk if a supplier's internal procedures are insufficient to prevent abuse of this access, or if there are technical weaknesses in the implementation of the remote access system. Currently, such connections are established through VPN links, but with very little logging and auditing of the specific equipment connected to, and actions carried out. The number of external connections to controlled networks will increase, both due to practical and business reasons. Connections to third party generation sites are one such example, where it is necessary for relatively simple communications to take place over an external IP network. While best efforts are made to assume the worst-case when considering third party networks, there is clearly potential for compromise here. There would be security benefits in having the capability to segment access to only a particular type of equipment, or localised site, to reduce exposure of assets to those with remote access. Care should be taken around legacy devices and protocols being introduced to IP-based networks, to ensure they cannot be reached from untrusted areas of the network, such as incoming VPN connections and similar.

The reliance of DNOs upon their supply chain of suppliers, vendors and subcontractors was recognised as being a major limitation of current cybersecurity measures. Questions were raised on how to audit, assess and review the cybersecurity competencies of third parties, especially while considering implementation-specific requirements or validation of vendor claims. There is also the issue of the validation of the supply chains of the vendors themselves. A code of practice for suppliers and other third parties, covering their expected capability in cyber security, was highlighted as an important requirement going forward.

Within substations, a significant concern identified was in managing suppliers' understanding of substation implementations and preventing inappropriate hardware from being installed in substation environments, where it is left unmanaged with security issues. For example, features that may be disabled on a product may still leave functioning remnants, capable of communication and remote exploitation.

The trade-offs and challenges of embedded systems were also discussed, specifically around short support periods from Original Equipment Manufacturer (OEM), which are often only a few years. The need for significantly longer equipment lifespans, causing vulnerabilities and weaknesses to get "locked in" with no clear way to mitigate or resolve them without OEM involvement.

**Inter-Organisational Issues.** There is a need to define collective responsibility across interdependent organisations, in order to secure energy systems and to ensure all market players and applications have achieved an adequate level of cyber-security. Aiming for a consistent approach across organisations will require collaborative agreements on cyber security responsibilities and increasing cyber-awareness both within and between organisations. Considering suppliers and components that affect the criticality of an operator and understanding security requirements in different operational contexts will help to adapt countermeasures to different use cases. With a better understanding of appropriate countermeasures, DNOs can agree obligations with suppliers to implement technical or organisational security measures and make plans to ensure compliance with those obligations. This could include a classification of threats, risks and vulnerabilities that indicates how essential certain measures are and the level of implementation required depending on criticality for the operator.

### 5.2.8 Recognising the shared context

It was important to bring together a shared understanding of the future energy situation through this research activity involving different players. Operational teams were getting to know new capability and new systems, learning an unfamiliar context. For example, keeping the power network stable involves controlling generation equipment on third party sites, managing Electric Vehicle (EV) charging patterns, so that power flows can be optimised within the constraints of the network. The resulting increase in complexity and data traffic, mean the availability and integrity of measurement data is essential to minimise unnecessary curtailment of generation. Agreement on cybersecurity requirements and code of conduct is also necessary between generators, DNOs, aggregators and other third-party providers.

The academic and industry experts participating in this research activity gained a closer understanding of the issues the DNOs face. This has provided a shared understanding from

which to design more applicable cybersecurity solutions and deployments going forward. Our multi-actor approach was able to consider the wider engineering solution, beyond security, for wider protection from undesirable consequences, especially where security is lacking. Knowing the operational perspective allows cybersecurity to be managed from an understanding of the organisational context.

Achieving security across organisational boundaries arose as a significant issue across several topic areas, including cooperation during incident response. The collective responsibility across interdependent organisations requires an adequate cybersecurity level across all market players.

During this Industry Review, the importance of organisational context was apparent, and it was clear that cybersecurity approaches and mitigations essentially must consider the operational and cultural context they need to function within.

## 5.3 Exploring Impact and Uncertainty

The FES all present an increased use of smart technology and therefore an increased exposure to cybersecurity risks. There are multiple dependencies on assurance decisions in the supply chain and across diverse actors. It is important to recognise and respond to risks across all interconnected stakeholders and elements so that threats are not missed at different points across those interactions. It is necessary to secure beyond just critical components with everything interconnected and a wide set of roles and technologies supporting the system. An integrated system inherits the security limitations of each interacting component. Transparency of assurance actions will be necessary where there is dependency on the cybersecurity maturity level of other actors.

Attacks are inevitable and are constantly evolving. By establishing clear responsibility for assurance and effective coordination across stakeholders, a broader protection across people, processes and technology can be attained. This would be aided by effective measures to evaluate the assurance of all components and their interactions and make sure appropriate areas are addressed across all aspects of the socio-technical system.

### 5.3.1 Impact Analysis

An exploration of impacts and consequences in a power system context was carried out, through interactions with industry partners and a review of literature [10] [64] [69]. Sharing an appreciation for potential consequences can give different stakeholders a reason to take the necessary action. Table 15 outlines a selection of potential impacts showing consequences of cyber events including data loss, data modification or unwanted control actions. There may also be indirect or unintended consequences involved in the system's response to a threat. Considering the system functions and how particular workflows and stakeholders are affected by the sequence of the threat through the technology, people and processes can help to uncover potential consequences of a threat.

Consider the roles, processes and underlying IT and OT technologies involved in delivering energy system functions, the assets and actors involved at each step in a business process. The flow of activities can be mapped onto components and interactions to identify the assets and actors [70]. This will build a picture of the systems, devices, communications channels, internal and external actors etc. that are supporting the functions [57]. The expected 'deep digitalisation' of assets [65] correspondingly requires a deep enough knowledge of system operation to know all the sources of control and automation and potential access pathways for attackers. Detailing the assets that contribute to essential functions and their impact if unavailable or compromised and from where changes can be made to configurations and settings [57]. The scale involved also changes the threat exposure i.e. how many instances of the data or device there are and if an asset is centralised or distributed [70].

A functional example such as operating within network constraints requires the secure retrieval of data from the network for real-time information on thermal ratings and voltage stability. This may also require access to smart meter voltage data or power flow and voltage information at DER connections. The cybersecurity of a 3rd party data centre or cloud service could also be a part of this flow of information. Threats to consider would include the unauthorised access or potential data manipulation of the SCADA monitoring and notifications of thermal or power flow constraints [71].

| Event | Consequences |
|---|---|
| **Temporary outages** | Activation of load shedding.<br>Tripping of protection.<br>Communications outage causing delay in data transmission/control actions. |
| **Affecting synchronisation** | Coordinating connection and re-connection of generators, without proper synchronisation could destroy generators. |
| **Resource Unavailable** | Denial of service attacks making a resource unreachable or unresponsive, and affecting data streams from devices e.g. phasor measurement data. |
| **Stealing data** | Extracting confidential information.<br>Social engineering to gain credentials.<br>Eavesdropping, sniffing IP packets, intercepting wireless transmission.<br>Side-channel attack to infer cryptographic keys from unintended information leakage. Impacting customer privacy, passwords, unauthorised access to systems |
| **Manipulation of data** | Injecting false data e.g. man-in-the-middle attack hiding true status from control centre.<br>Modifying data e.g. tampering with sensor data to cause inappropriate load management resulting in unnecessary load shedding or generator trip out.<br>Manipulating measurements.<br>Undesired system behaviours. |
| **Unauthorised access** | Access to private data.<br>Identity spoofing, impersonating an authorised user e.g. man-in-the-middle attack, message replays.<br>Intrusion affecting behaviour of system e.g. via open ports or malware. |
| **Unintended Consequences** | Unknown consequences aggravated by evolving threats and interdependencies across diverse actors. |
| **Sabotage** | Embedding malware to launch an attack later. |
| **Asset replacement** | Considerable lead times for replacing destroyed assets. |

Table 15 Potential impacts of cyber attack

The resolution of network constraints being either demand led or generation led would require secure access to flexibility resources for service activation or dispatch. The cybersecurity of control actions in the actuation of DER, aggregator services or active customers would need to minimise the risk of inappropriate control actions or unauthorised access. The assessment of the operational performance of flexibility services could require cybersecurity performance to be included in their reliability metrics [71].

Mapping the entire thread of activity for energy system functions onto the supporting processes, assets and roles in this way presents the impact of threats on essential functions. The aim is to apply mitigations to protect these functions and minimise the impact of events.

## 5.4 Resilience Efforts

To improve resilience across interdependent actors, cybersecurity expectations and requirements appropriate to each actor will need to be defined and agreed for: [71]

- Aggregators supplying services to the power grid via DSOs from assets on the distribution network.
- Active customers and developers exporting power to and importing power from the distribution network.
- Increasing volumes of Distributed Energy Resources with connection arrangements via distribution networks, the cybersecurity aspects of their operational role and their participation in markets via DSOs or aggregators.
- Combined approaches for supply chain actors to engage with multiple DSOs.
- Transmission connected demand and generation, with cybersecurity and resilience actions included in their connection agreements.

Resilience efforts across all actors need to include activities such as:

- Testing changes to assets for cybersecurity or operational impact before deployment.
- Managing access and identity across human and IoT actors.
- Involving stakeholders in threat and vulnerability management for access to a more thorough threat landscape.
- Coordinating incident response activity with appropriate external entities.
- Constructing evidence, contracts and SLAs with third parties.
- Assigning and managing cybersecurity responsibilities across personnel and all relevant stakeholders. [72]

Each stakeholder will hold a different level of interest in contributing to system resilience and differing degrees of influence on the cybersecurity level of the system. Considering the

relative positions of different stakeholders would reflect how best to engage each actor in required resilience actions.

To know and measure operational resilience requires defined and implemented processes. Processes offer the context for how to achieve a resilience activity with specifics related to roles, technology and operations. The processes that contribute to resilience need to be performing well to build a confident state of readiness in the face of new and different threats and risks. The supporting assets and interactions that enable the functionality of smarter grids need to be cybersecure and reliable. Processes aiming for operational resilience need to be embedded within functional activities to improve the security and resilience of essential services [73].

Reporting on assurance actions across organisations may be necessary where there are dependencies on other actors to deliver a function or service. Preparing combined resilience actions and measures per function would help to define clearer responsibilities for assurance and effective coordination across stakeholders.

## 5.5 Interdependency in Future Energy Contexts

This work enabled a thorough observation of the cybersecurity situation for the energy sector by inviting insights from different perspectives to be shared. The energy system is evolving into a complex web of demand and supply across diverse actors. It will increasingly rely on the security of the information infrastructure supporting it, and the resilience of a digitalised operating environment. To make sense of the latest threat landscape requires a wider sharing of knowledge and awareness among all stakeholders for organisations to make better informed decisions and actions. To construct a picture of the latest operating conditions and vulnerabilities requires knowing the resilience of different assets and interactions that make up the functions of the energy system. Along the thread of activities required to deliver each function, a change in vulnerability in one area could increase the threat affecting other areas. The number of instances of a vulnerable component will affect the scale of threat a function is exposed to. Processes and measures that allow for a greater transparency of cybersecurity activities will encourage preparations and build the necessary trust across interconnected stakeholders. This will enable a more robust response to changing events on the system.

This research has provided a thorough investigation of cybersecurity issues and concerns for utilities to provide an organisational and future energy system context for the ongoing design of cybersecurity improvements. Methods and approaches have been recommended for improving resilience across interdependent actors and to minimise the impact and consequences of cyber-attack. With smart digital technology deployed at scale, cyber governance must provide an essential foundation for our future energy scenarios with the capability to, repeatedly and reliably, assure the integrity of interconnected systems and users.

This foundational work also enabled future cybersecurity projects at PNDC including improving incident response capabilities, asset discovery on power communications networks, identification and analyses of vulnerabilities in network assets and penetration testing of electric power assets.

This work led the author to continue researching the inter-organisational issues that were raised. To further explore stakeholder perspectives and the building of trust among them, Section 6 provides a case study of public private partnership in the European energy sector.

# 6 Public Private Partnerships (PPP)

This chapter describes the formation of a partnership in cybersecurity cooperation across national borders and the utilisation of practice spaces within this group to progress collaborative working. It includes an analysis of the first year of experiences with implementing the NIS Directive, that was provided as feedback to policymakers.

Multistakeholder partnerships enable transboundary interactions between public and private actors in the interests of a common good. Public-private 'partnerships' are often described as being a 'cornerstone' of cybersecurity however clear lines of responsibility and accountability need to be defined as each side of the partnership has its own perspective. The private sector emphasises economic promotion and pays closest attention to the financial and reputational aspects of cybersecurity, while the public sector retains responsibility for national security [74]. With most of critical infrastructure being privately owned, the combined provision of security by public and private actors requires a clearly defined arrangement. The assumption that the private sector can invest in cybersecurity "beyond its cost/benefit analysis… to ensure national security" requires some oversight to achieve the required level of cybersecurity. Furthermore, a company's risk appetite may or may not align with the government's perspective on national security as a public good [74].

There are key and potentially complementary differences in focus between government and private sector cybersecurity requirements. From a government perspective there is a need to assure the cybersecurity of essential services that are provided over privately owned Critical Infrastructure (CI) [75]. Government interest tends towards defence of the nation and the attribution of perpetrating actors. Their view is more outwardly focussed towards threats, including those from other states or state-sponsored actors. Conversely the private sector is more inward looking and focussed on vulnerabilities. Their attention is on the inevitability of cybersecurity risks and balancing those alongside other business risks. A private actor's inward view is to detect, mitigate and foster their ability to recover from attack. Awareness of a company's reputational risk has also brought more emphasis to cybersecurity preparedness. The goals of privately owned infrastructure being organised for profit can be inconsistent with the goals of privacy and security with investment in cybersecurity being influenced by budgetary considerations acting to reduce

costs. This gap in agendas opens up opportunities for cybersecurity risks to manifest [76]. Embracing the diverse perspectives of public and private sector participants is important and can bring “many different threat realities and approaches” to the table [77]. “The most effective cybersecurity solutions will inter-relate stakeholder requirements at multiple system levels.” [76] Cybersecurity responsibilities to be met by private assets implies a “diffusion of authority from government to public-private implementation networks” [78].

The concept of cybersecurity as a shared mission and the reality that “no single management entity has control over the whole” [79] has encouraged Public-Private Partnerships (PPP) or Information Sharing and Analysis Centres (ISAC) to form, enabling government and industry to work together. Governments need to achieve an acceptable security level for their nation from a mix of different private sector responses to the risks. Cooperation across these different responses allows a broad and flexible understanding of shared risks, enabling continuous adaptation “to the benefit of both the individual partners and the common good” [77].

In cybersecurity, PPPs have been shown to be based on more than a strategic self-interest and management of reputational risk. There is a social glue that binds these partnerships with professional loyalty, founded by higher moral principles. This gives a subtle power of commitment and loyalty to these partnerships that goes beyond simple strategic interests. Embracing the different perspectives from diverse participation also gives value to the PPP. Such partnerships bring “a commitment to future commitments” [77] often through voluntary contribution and going beyond immediate results without specifying outcomes. This commitment requires:

- Openness and trust.
- Shared understanding of risks/threats requiring mitigation through collective effort.
- Collaboration for new solutions to a common purpose.
- Long term relations [77].

Such partnerships and collaborations provide an important foundation to assemble and discuss the requirements of government and the private sector. Prioritising

interconnectedness and dependencies to achieve the required capability, while acknowledging the limits to cooperation where interests of government and private actors are more disparate. The discourse on PPPs explores how to make the private sector more like government with respect to the values applied to it. Business imperatives do not always align with public values, so it is recommended to focus on preserving values in specific contexts and circumstances [80]. The public-private cybersecurity system demands greater vigilance from a broader range of stakeholders. Operation of cybersecurity governance has become more diffuse and more complex, reliant on a mutually beneficial pursuit of interests by both private and public sector participants [80]. The following case study serves to demonstrate private actors playing a useful role in fostering public values to protect grid networks and energy services. This study provides evidence-based analysis of the formation of an ISAC collaboration, highlighting essential aspects that assisted a successful ISAC to be built and the challenges faced by such a group.

## 6.1 Case Study - Establishing an Information Sharing and Analysis Centre (ISAC)

ISACs are associations designated for sector specific information exchange on cybersecurity incidents [81]. With the aim of improving cybersecurity in independent industry areas, they often interlink industry and governmental organisations, forming public-private partnerships. For more effective decision making in preparation for and response to cyber events in the energy sector, multilevel situation awareness, from technical to strategic is essential. With an uncertain picture of evolving threats, sharing of the latest cybersecurity knowledge among all sector stakeholders can inform and improve decisions and responses. ISACs attract members from utilities, suppliers to utilities, cybersecurity solution providers, academia and research organisations.

The EU Cybersecurity Strategy 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 sector as being crucial due to a government's duty to protect critical infrastructure that exists within the private sector [82].

A European funded project, DEnSeK (Distributed Energy Security Knowledge), proposed an Energy ISAC with opportunities for information sharing and to build a situational awareness network for the energy sector [83]. Following on from the DEnSeK project, this study examines the formation of a European Energy – Information Sharing & Analysis Centre (EE-ISAC) defining the approach and methods used.

Coordinating the start-up stage of an ISAC enabled an academic contribution to be developed alongside practical progress. This action-focused research implemented the prototype of a first cross-border ISAC for the energy sector, while fostering cooperative partnerships in cybersecurity. The EE-ISAC is now used as an example ISAC for other sectors and their learning and experience is often used to inform the formation and development of newer ISACs.

The development of EE-ISAC towards regular information sharing among members is here described demonstrating the foundations achieved so far upon which a situation awareness network can be built for the energy sector.

### 6.1.1 Governance & Strategy

To define the direction and approach for the new ISAC, the EE-ISAC Management Board held several conference calls and an in-person working session ahead of the first member plenary. Board meetings were held monthly via conference calls and a face-to-face Board meeting ahead of each member plenary, to set the direction and agenda for the plenary and ongoing working groups.

A Mission statement was decided:
'To improve the resilience and security of the European energy infrastructure. We do so through trust-based information sharing and by enabling a joint effort for the analysis of threats, vulnerabilities, incidents, solutions and opportunities. EE-ISAC offers a community of communities to facilitate this proactive information sharing and analysis, allowing its members to take their own effective measures.'

The key strengths that would be fostered by the ISAC were defined as:

- Sector specific intelligence across the energy value chain.
- Engagement of a variety of sector Stakeholders.

- Access to a broad network of organizations.
- Proactive and Trust-based Sharing Community.
- Enhancing organizational resilience and preparedness.

Five key success factors for EE-ISAC were decided each with a Management Board member as sponsor. Groups were created to coordinate the success factors with a deputy from the members to help guide this success factor together with the sponsoring management board member.

1. Breadth of members and membership criteria: To consider the total energy value chain, aiming for involvement of all energy domains in the ISAC to create a balanced group. This group was to focus on attracting those other parties to join the ISAC.
2. Strategic ISAC collaboration and partnership: Formalizing collaboration and partnership with other ISACs. This was to include energy sector partnerships with ISACs in other nations as well as connecting across sectors with other European ISACs.
3. Analysis of threats, risks and incidents. One of the main reasons to create this association was to help each other, share information and to provide early indication and guidance on how to protect our own organizations. This group attracted several member volunteers to begin the activities.
4. Information sharing platform activity including webinars. Aiming to join all members through a confidential sharing platform and to provide webinar discussions in between face-to-face meetings.
5. Useful reports: To create useful reports through sharing expertise, experiences and analysis, with an emphasis on quality and relevance of the reports rather than a regular quantity.

### 6.1.2 Membership and Trust

The original vision of EE-ISAC was to join forces across the whole energy supply chain and improve awareness among all stakeholders, however representation in the ISAC depends on who chooses to join. Various mechanisms and incentives have been put in place to ensure a balance of participants. During the development of EE-ISAC it has been necessary to encourage the participation of utilities to keep EE-ISAC's work and approach tailored towards the needs of energy utilities and the context of operating a power system. A utility presence

has also been maintained in the leadership team, with always 3 out of 5 Board members coming from utility organisations. Along the way, there have been decisions by the Board to monitor and redress the balance of members by pausing membership requests from non-utility organisations until more utilities are recruited. While it was frustrating to have a queue of interested members waiting, this helped the marketing effort to keep up the goal of having a utility focus.

Multi-stakeholder partnerships have been viewed as problematic where voluntary governance arrangements can privilege more powerful actors. This has been evident in sustainable development partnerships [84]. Such partnership experiences have warned of power differentials with larger players wielding a greater influence [85]. Indeed, larger utilities have been more forthcoming with commitment to join the EE-ISAC, having more resources to give time to the ISAC and pay the membership fee. However, a gathering of experience to share with smaller utilities has also played out. Awareness of this situation spawned one of the working groups set up to pool experiences in incident response from the ISAC members. A white paper was produced to create content for smaller utilities without resources for IR and without the chance to join the ISAC [86]. The good understanding of dependency on other actors within the power system appears to encourage better interworking between potentially impacted players.

The purposeful leaning towards an appropriate balance of utility members and leadership by utilities was to ensure the tailoring of cybersecurity guidance, analysis and expertise towards the context of an operational environment and to integrate cybersecurity with a strong understanding and experience of operating the power system. The growth of ISACs have also been supported at an EU level. Membership of and participation in an ISAC is seen as favourable within EU funding mechanisms to encourage the knowledge from implementing cybersecurity improvements to be shared with other ISAC members [87].

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 of the EE-ISAC space to grow among the same people attending meetings regularly. The

representatives are required to sign confidentiality agreements and the full membership are given three weeks to approve the joining of new members. As a result, close working relations have gradually been established, to develop and encourage sharing of sensitive information during EE-ISAC's closed member only meetings.

The careful building of a trusted network was an essential foundation to ensure the effective and appropriate use of platforms and tools offered by EE-ISAC and a willingness to engage with the unique collaborative opportunity that EE-ISAC offers. As far as the progress achieved with building membership, creating partnerships and forming working groups is concerned, 28 representatives of utilities, vendors, public bodies, academia and research labs have signed the membership, 10 practice groups have been established and mutual agreements have been signed with 9 partners.

### 6.1.3 Information Sharing

In addition to holding regular member meetings, a digital sharing platform was launched, shown in Figure 11, and configured for the needs of the group. The author administered this platform and created spaces for different practice groups to interact on chosen topic areas. Members appreciate the added value of EE-ISAC as a forum for discussing relevant topics and issues they all face. It was important for the group to have its own online presence to continue working and sharing together between meetings, including regular posting of new information on threats and vulnerabilities.

The author's experience of the ISAC's use of this platform was provided to the Empowering EU ISAC project for new tool development applicable to all ISACs. The intention of the new EU ISAC tool was to encourage information sharing within a single organization to mainly share information and analysis among ISAC members, but 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 is to be taken into consideration in a future version.

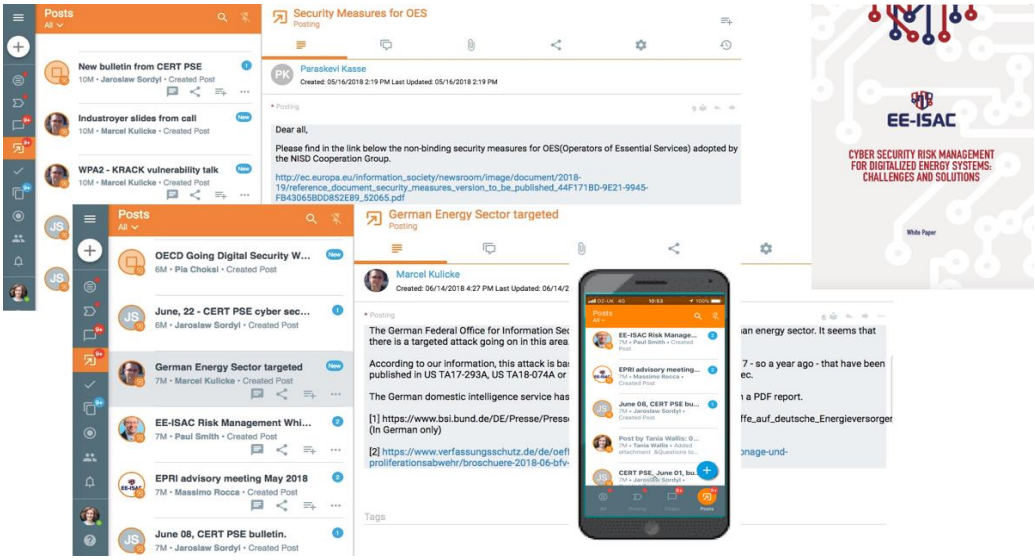


Figure 11 EE-ISAC's information sharing platform at work

EE-ISAC is forming its own instance of malware information sharing tailored especially for the energy sector (see Figure 12) that implements the concepts described during the DEnSeK project [88]. This is being progressed by EE-ISAC's threat intelligence working group, described in Section 6.1.4, to become available to all EE-ISAC members to both contribute to content and receive the latest information.

This is providing useful input to the decision process by sharing information about ongoing threats and artifacts in quasi real time, assessing if detected activity is malicious activity. 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 for critical infrastructure operators. This combined effort of EE-ISAC members is working towards building sufficient intelligence sources and aims to enhance it with interesting outlooks on threat trends and attack schemes affecting the energy sector. The analysis also holds potential to provide earlier indications of future risks.

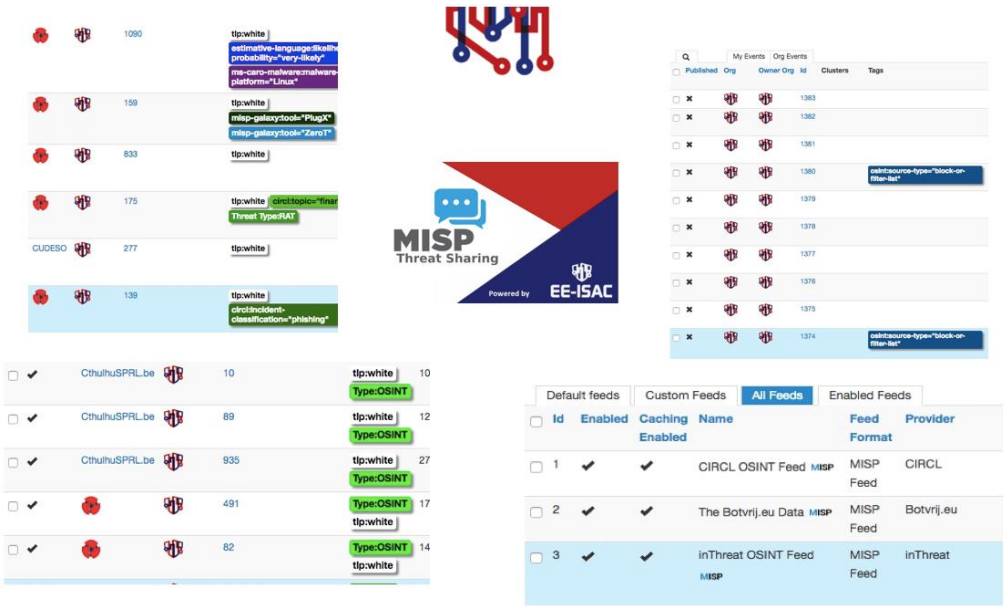


Figure 12 EE-ISAC threat sharing

### 6.1.4 Practice spaces within the ISAC

Essential topic areas were chosen and several technical practice groups were formed to commence specific collaborative activities. This enabled focussed communities to work together on the current issues, as displayed by Figure 13.


Figure 13 EE-ISAC communities and practice spaces

At the fourth plenary, the following topic areas were proposed to encourage In-Kind Contributions from members:

1. Education and Awareness.
2. Incident Analysis & Threat Intelligence
3. Governance Privacy & Security
4. Cyber Physical Security
5. ICS/SCADA vulnerabilities
6. Risk assessment/management
7. Solution and services
8. White papers

The author commenced practice space activities, applying the approach described in Section 2.1, to launch actions on the above topics. Inviting contribution to the issues, an achievable vision was developed with each of the groups, the aims for each group were decided and presented to the membership at the fifth plenary to encourage further input. The ongoing development of these practice groups was dependent upon member interest and availability to contribute, therefore some practice spaces progressed further than others. As administrator of the EE-ISAC information sharing platform, the author created small group sharing spaces on the system for these practice groups to work together between meetings. The practice spaces aimed towards delivering a useful contribution to utilities and were mostly made up of EE-ISAC members. However, non-member input was also invited to contribute specific expertise where needed by the group.

### 1. Education & Awareness

A community for Webinars and Round Tables was created on the EE-ISAC portal, open to all members to join. This group is hosted by ENISA with members deciding and voting for topics and themes for the webinars.

The aims set for this group were to:

- Raise awareness of cyber security.
- Create opportunities for information sharing and cooperation.
- Make an educational contribution to the energy sector on cyber security and resilience.

- Help members keep up to date.
- Attract potential new members.
- Create 2 or 3 meaningful webinars each year.

The different audiences for this work to reach are:

- Internal, for members only.
- Inviting potential new members.
- External eg through providing some access to webcasts in the public area of the EE-ISAC portal.

During the founding years of the ISAC the below topics were presented to members:

- NISD introduction and later a NIS Directive update.
- ICS/SCADA security tools.
- GDPR and Data Protection Impact.
- Interdependencies for energy operators.
- Industry 4.0.
- Secure Substations.

Members continue to be encouraged to offer ideas and content for webinars. This working group has evolved to provide more interactive sessions, encouraging live discussion on topics such as:

- What is the best build-up of a SOC for utilities?
- Electricity sector Cyber Capability Maturity Model C2M2.
- Securing the human element – how to prepare your organisation against phishing attacks.
- Discovering and defending against vulnerabilities in building automation systems.
- How embedded TCP/IP stacks breed critical vulnerabilities.

In addition to webinars, ENISA offered training on how to set up monitoring, forensics, attack detection and analysis in an ICS/SCADA environment. EE-ISAC also contributed to ENISA's toolkit created to support the establishment of ISACs in all critical sectors.

A utility member hosting Incident Response training with GridEx extended this opportunity to other ISAC members, an opportunity for ICS cyber exercises in Europe equivalent to the bi-annual NERC event in the US.

### 2. Incident Analysis & Threat Intelligence

A central working group essential to the ISAC was to build threat intelligence tailored for the energy context. Initial aims at the beginning of this working group were to:

- Confirm the core team, encouraging participation from utilities, to include appropriate operational and technical skillsets.
- Set the initial topics, define & approve methods to be used.
- Outline the results of investigations as Best Practise, reported and presented to members.

An information sharing system was proposed to facilitate threat intelligence. A technical pilot was arranged for the curation of threat intelligence tailored to the Operational Technology (OT) community. An overview of the MISP Proof of Concept project was provided to members in order to discuss the approach, including setting up the infrastructure, which partners/servers to integrate with the platform, finding points of contact who could assist with next steps, support gathering data on the platform and testing connections with sharing groups. There were also access arrangements to make including administrator roles and rules for sharing. It was envisaged that bi-directional exchange would be possible the following year.

Initially, during the set-up period, the use of MISP was facilitated among the Threat Intelligence (TI) working group before being available to all members. This core TI working group was made up of 70% utility members and was responsible for checking the application and features first and confirming the information feeds going into MISP, agreeing procedures and criteria, before the platform access was opened up to further interested members. The core team were contributing to the content and other members were later receiving information through access to the consumption area of MISP. Eventually 55 threat intelligence sources were integrated into MISP and a vetting process for 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 use of the tool to share information and to perform better analysis on threat trends, to help operators identify false positives and have a more structured collection of events.

Following the simulation phase and with new user accounts set up, the EE-ISAC MISP service was launched. The next stage will reach out to other partners such as E-ISAC and X-ISAC

(cross sector ISAC community) to connect MISP platforms and also to integrate with the MISP of EE-ISAC members. Members are to discuss how they will leverage the capability of this platform and aim to facilitate this stage through a monthly call and interactive sessions with the platform. This working group also provided a White Paper on Threat Intelligence Management. This has become a living document to share new approaches over time [89].

A workshop was held at a member Cyber Range to investigate incident response processes together and define best practices for the OT environment. Several members contributed content to an Incident Response White Paper during and following this workshop. The outputs from the workshop provided content that is specific to the energy sector [86].
ENISA have created a threat landscape report for the energy sector and continue to produce an updated threat landscape report annually. EE-ISAC members are invited to contribute to this report.
At the last in-person plenary, a new working group was proposed to make phishing campaigns a topic for a future meeting and webinar. It was also suggested to form a working group to gather insights from a utility spear phishing program and best practises from partners, with the aim to develop some guidance through a white paper on phishing.

### 3. Governance Privacy & Security

An open community was created on the portal to offer support to members on GDPR and issues relating to privacy and data protection. This group set out to:

- Encourage ongoing sharing and discussion on EE-ISAC portal.
- Collate common issues and concerns with GDPR.
- Assess the impact of GDPR.
- Interpret regulation measures for utility sector.
- Analysis and Classification of data to identify critical data to protect.
- Seek support from academia for privacy and data protection improvements.
- Hold a workshop to help members to move forward with GDPR.
- Decide potential scope for a white paper.
- Create webinar to explain topics.

This group began moving forward in realistic steps, launching one topic at a time, the first topic suggested being: Data Protection Impact Assessment (DPIA). Members that were contributing to regulatory recommendations for privacy and data protection were able to

present the outputs from this work during plenary discussions on this topic. This included providing a walk-through DPIA of smart grid and smart metering systems [70].

### 4. Cyber Physical Security

All members were invited to propose topics and help develop content. Several topics were suggested including:

- Distant maintenance in IT/OT environment.
- Secure Substation IEC 62443.
- ISMS IEC 27001 certification.

Suggestions given on the approach for this group were to:

- Gather together members working on substation security.
- Look to vendor companies for expertise, eg Schneider info on substation security.
- Explore the potential to open up working groups to influence standards.
- Collect information on topics to refine into a summary white paper, identifying sources to go deeper.

While initial aims were for 2 to 3 publications per year, time and resources to commit to this were not forthcoming. However, this group enabled confidential information sharing on substation security and greatly assisted in establishing the culture of regular trusted sharing sessions during member plenaries.

### 5. ICS/SCADA vulnerabilities

The aims for this group in the first 6 months were to:

- Produce a whitepaper on Ransomware
- Run a workshop to raise awareness.
- Provide some guidance on how to proceed in the face of vulnerabilities.

Suggestions for way forward:

- Identify synergies with threat intelligence working group and secure substation effort.
- Identify vulnerabilities specific for the power sector, which are targeting ICS.
- Input to research where need to go deeper. Form a group of 6 to 8 companies for deeper investigations.
- Consider the full attack surface including insider threat.

- Survey questions from members to focus the study.
- To access colleagues within member organisations where specific expertise is required i.e. interaction beyond the two EE-ISAC representatives per member organisation.
- Create a Project description with plans for conference calls and next steps.

This group began collating a report to include:

- awareness of ICS/SCADA vulnerabilities and how to rank them.
- mapping of threats to know if vulnerable.
- support for Utilities on how to deal with vulnerabilities.

Outputs were presented to a member plenary and feedback requested on what case studies could be taken further. Specific contributions were later provided through webinars.

**6. Risk Assessment/Management**

This group benefitted from research expertise from recently funded projects in Risk Management so positioned themselves to

- offer guidance on methodologies based on experience.
- look to operators to consider their skill gaps and requirements for guidance.
- Prepare documents together and provide material on portal.
- Produce webinars from existing material available from members' project outputs.
- Produce a white paper together covering:
    - Best practises and experiences.
    - Pitfalls and how they were addressed.
    - Skills required to deal with risks.

A white paper on Risk Management for Digitalized Energy Systems was produced to bring together contributions from three recent cyber security projects, SPARKS, SEGRID and HyRiM that all included a component of risk management [90]. The intention was to produce an introduction to the topic, pointing to other material for more detail. Feedback from the wider membership was invited to help shape this work to be more applicable to utility requirements. When the final version of the paper was presented at a member plenary, interest was shown in taking this work forward with some practical applications.

7. **Solution & Services**

This group was to consider the potential for producing a regular threat intelligence newsletter for the energy sector. A utility member began providing a weekly threat intelligence report which all members found to be very useful. Communicating the evolution of threats previously used in power grid attacks, helped to identify early stages of multi-stage attacks. Understanding attack models and adversary behaviour has offered assistance to better mitigate. Another member has presented, annually, their ICS/IIoT threat report to members ahead of publication, a compilation of their experiences working with ICS organisations.

8. **Academia & Research**

Academia members shared their current research domains to consider potential areas for collaboration. Goals were set to produce white papers in these chosen domains and to support other EE-ISAC working groups. It was proposed that a discussion be opened to consider closing the gap between research and industry by understanding better the needs of utilities that could be met by research projects with specific help. A number of papers were produced with academia at the centre of the collaboration including the Risk Management and Incident Response white papers and a journal paper on Realising the EE-ISAC [90] [86] [91].

EE-ISAC and the Electric Power Research Institute (EPRI) explored the potential for a sub-group of EE-ISAC members to implement cybersecurity metrics. EE-ISAC had proposed a benchmarking exercise for members to compare their maturity levels and showed interest to work in collaboration with EPRI to monitor the progress of this initiative by using EPRI's metrics. EE-ISAC needs to choose a maturity framework for this exercise. As a starting point a subset of indicators were proposed from EPRI's metrics research [92] and a connection established to their Metrics Advisory Council for technical expertise and regular updates.

### 6.1.5 Forming partnerships

Significant attention has been given to marketing and membership, to attract relevant members and partnering with expertise to bring value to the members and to the energy sector. International links were established during the early stages of building the ISAC. An expert in protection of critical infrastructure from the North American Electric Reliability

Corporation (NERC) and the US Electricity ISAC was invited to the first plenary, to give advice on establishing the ISAC as an information hub for the European energy sector. Discussions with Japan also began at this time, to share the EE-ISAC model, when there was interest to set up a Japanese Energy ISAC. Then a Tri-lateral Memorandum of Understanding (MoU) was agreed and signed between EE-ISAC and Japanese JE-ISAC and U.S. E-ISAC. As well as attendance at EE-ISAC plenaries, the tri-lateral partners have participated in the annual GridSecCon and GridEx events. US E-ISAC have been growing their organisation to offer faster response and stronger information sharing. They initially had in place a 12 hours x 5 days operations facility and then increased that to 24 hours x 5days on-duty watch. They recently expanded further to cover 24 hours x 7 days on-duty watch operations by end of 2020.

A first stage baseline for tri-lateral information sharing was for all three ISACs to start sharing basic system information at first to identify similarities among systems in Europe, Japan and USA and to get to know the kind of incidents most relevant to share. The partnership aims to share indicators of compromise such as attacker IPs, patterns etc and general information on targeting of energy-sector relevant equipment or supply chains. Following significant events, such as ransomware, there has been engagement to share experiences. A Traffic Light Protocol (TLP) cross-check exercise was initially carried out to harmonise TLP definitions between the three ISACs to indicate whether information can be shared with ISAC members, trusted parties or publicly [93]. Japan E-ISAC willingness to attend in person events and increasing sensitivity to cyber security risks, during the lead up to host the Olympics in 2020/21 helped to invigorate the tri-lateral partnership.

The author created a small practice space between the three ISACs to encourage the relationship towards regular sharing on topics of interest. A chance to discuss the relationship and progress with contributions assisted in moving from a formal connection between ISACs into active interworking and a regular rhythm of sharing events. There has been a noticeable increase in information sharing and willingness to connect during 2021 with US E-ISAC sharing ‘more than ever before’. The ISAC partners offered access to each other’s information sharing systems and a timeline of quarterly information sharing meetings is now established with monthly informal catch-ups to maintain connection and progress the partnership.

An MOU was also established with a Norwegian cybersecurity organisation KraftCERT who are also part of the Forum of Incident Response and Security Teams (FIRST). KraftCERT have a network of partnerships in place including a community of CERT organisations giving potential for EE-ISAC to link with their established alert function. More recently partnership agreements have also been made with Eurocontrol in the aviation sector and a global OT-ISAC based in Singapore that is linked with the Global Resilience Foundation (GRF). EE-ISAC already had in place a partnership with the GRF's intelligence sharing community for the energy sector Energy Analytic Security Exchange (EASE) with access to their portal and regular bulletins.

The EE-ISAC participated in and contributed to regular inter-ISAC meetings with other sectors (X-ISAC), hosted by ENISA. A new partnership with the European Rail ISAC (ER-ISAC) has evolved and EE-ISAC have recently contributed to a road map review to define working groups for the ER-ISAC together with peers in Aviation and Maritime. EE-ISAC has also supported the development of ISACs in other regions through the US Agency for International Development (USAID), including an ISAC for the Black Sea region. The network of partnerships continues to grow with further agreements in progress with the European Network for Cybersecurity (ENCS), European Distribution System Operators (EDSO), European Utilities Telecom Council (EUTC) and Israel NGO 'CyberTogether'.

## 6.2 EE-ISAC Formation & Progress

The formation and progress of the EE-ISAC working group activities, evident at regular Plenary meetings, is described in Table *16*. Progress was very much dependent on the time commitment of members and availability to contribute. A sense of belonging grew through the core attendance at regular face-to-face plenaries, and this encouraged some progress with shared projects in between meetings when time allowed.

| **Stages of the ISAC** | **Activity achieved** |
|---|---|
| 2015 stakeholder meetings Lisbon & Nederland | Discussion of Articles, creation of EE-ISAC as a legal entity.<br>Agreement of Terms of Reference.<br>Election of Chair and Board Members. |
| Plenary 1<br>Rome 2016 | Adjust terms of reference to permit some Government Organisations to provide 'services in kind' instead of a membership fee, to encourage academic members. |

| | |
|---|---|
| | Discussion of Ukraine incident.<br>Connection with international partners in US and Japan commences. |
| Plenary 2<br>Virtual 2016 | Financial arrangement, opening of bank account.<br>Discuss marketing approach to attract members.<br>Report on Ukraine incident reviewed and shared.<br>Plan upcoming plenary presentations introducing GDPR and NIS. |
| Plenary 3<br>Porto 2016 | Define the direction and approach for the new ISAC.<br>Share Mission Statement, Key Strengths and Success Factors decided by the Management Board.<br>Create groups to coordinate the success factors. |
| Plenary 4<br>London 2017 | Defined 12 “in kind” contribution topics were proposed by the Board. |
| Plenary 5<br>The Hague 2017 | Eight technical practice groups had been formed, the progress and plans for each were communicated and discussed.<br>An intense and useful discussion and sharing following the WannaCry incident. |
| Plenary 6 Athens 2017 | Two utility members being willing to unpack and present their company’s experience and response to the Wannacry incident set the stage for a culture of sharing at member plenaries. The confidential sharing session was becoming a centrepiece of plenary events.<br>After an ambitious launch of working groups at the previous meeting, tensions arose on how realistic the expected outputs were for a voluntary association and some expectations diminished accordingly. At this point webinars and discussion opportunity in between in person meetings were valued more than documenting experience and best practices. |
| Plenary 7 Madrid 2018 | New utility members brought fresh ideas and enthusiasm for the ISAC. Contribution to producing outputs increased and weekly threat intelligence sharing began. |
| Plenary 8 Glasgow 2018 | This event attracted attendance from a wider network, including WEF and ECSO and DG Ener. The ISAC’s first White Paper on Risk was circulated. Prospective new members attended.<br>By this stage the Plenary had evolved into two different events, a marketing event with wider reach and a members only meeting. The enthusiasm towards marketing the ISAC had to be balanced with ensuring opportunities for members. It became important to protect a space for the member community with a closed event to nurture the building of trust and provide a suitable circle for confidential information sharing. At this members only meeting the MISP proof of concept project was presented, and next steps discussed. The chosen theme on substation security enabled presentation and discussion among utilities, vendors, and solution providers.<br>Ahead of each meeting an appropriate theme was selected and utility members invited to come prepared to share on that topic. |

| | |
|---|---|
| | This helped to facilitate a supported and productive sharing session at each meeting. |
| Plenary 9 Brussels 2018 | An emphasis on Global partnerships, including a video link to signing ceremony in the US between US E-ISAC, Japan E-ISAC and European Energy ISAC, and reporting on progress with supporting the development of new ISACs. |
| Plenary 10 Brussels 2019 | Feedback on implementation of NIS Directive presented to NIS Cooperation Group's Energy Workstream.<br>Annual ICS/IIoT Threat report presented to members. |
| Plenary 11 Warsaw 2019 | Live demo of EE-ISAC's MISP platform to show structure of event collection and analysis capability.<br>The idea to share incident response skills with smaller utilities encouraged the beginnings of a White Paper and a workshop designed to bring experiences together and tailor information to the energy sector. |
| Plenary 12 Athens 2019 | Members input to ENISA's annual energy threat landscape report.<br>Training on Network Forensics for an ICS/SCADA environment.<br>Output reviewed from workshop on best practices in incident response.<br>Quarterly meeting agreed and planned with EE-ISAC US E-ISAC and Japan E-ISAC to action regular information sharing between the tri-lateral partners. |
| 2020/2021 | Online Plenaries were held and gave the chance to review the progress of the ISAC, develop a forward strategy and participate in the Empowering ISACs project and cross-sector ISAC activity, to develop improved tools and support for ISACs (described further in Section 7). |

Table 16 EE-ISAC working groups formation and progress

## 6.3 Tool selection

During the start-up stage of the EE-ISAC there was a dependence on voluntary effort from members to progress most things at that time. Therefore, the selection of information sharing platform came from member experience and investigation of different platforms for their own use. There was also a cost consideration so the best option, in terms of affordability and functionality, was selected after exploring the platform capability to ensure it was a step up from other tools previously used. There was a considerable implementation effort involved. The author set up the different practice group sharing spaces on the new platform, arranged training for all the members and oversaw the transfer of previously shared content to be available on the new platform. From the author's experience of platform use by the ISAC, requirements were later fed into the EU Empowering ISACs project to create new common tools to support all EU ISACs that will be managed by ENISA going forward.

EE-ISAC's threat intelligence working group also created an energy sector specific instance of Malware Information Sharing Platform (MISP), a familiar platform with scope to be tailored towards the needs of energy companies. In essence, EE-ISAC was dependent on members volunteering ideas and exploring those options on behalf of EE-ISAC, rather than having a formal selection process that would have taken more time and money.

## 6.4 Analysis of NIS implementations: Experiences of Energy Operators

### 6.4.1 Summary of Responses

Responders were submitting anonymous feedback, so the information provided has been combined without exposing individual member responses. The compilation of feedback was reported to the NIS Cooperation Group Energy Workstream through the general themes appearing across all responses. These themes are described in the following sections to represent the experiences gained by energy operators while implementing the NIS Directive.

#### *6.4.1.1 NIS Directive published guidance*

The NIS Directive published guidance is generally seen as adequate. A more energy centric approach would be helpful to include more energy sector specific guidance, especially to assist in identifying NIS-relevant assets.

#### *6.4.1.2 Criteria for identifying an OES*

There is some inconsistency across different countries in identifying OES. In some places it is clear and each OES has been contacted by their public authority. In other countries, the methodology for identifying an OES is still work in progress.

#### *6.4.1.3 Clarity of reporting thresholds & notification schemes*

Notification and reporting thresholds need to be adapted to the specifics of each sector. Deciding on the 'Significance' of an incident's impact can differ across members states and sectors. There is limited understanding on how the NIS Directive will actually be enforced and the role of national energy regulators and NCSCs.

#### *6.4.1.4 Clarity of the latest cybersecurity issues*

Many different sources of intelligence are giving different information - a more centralized view of the latest issues with appropriate and sufficient details to respond would be helpful. Security responsible authorities seem to be relying on reporting from OESs and offering little feedback on the latest threats.

#### 6.4.1.5 *Actionable threat intelligence*

Threat intelligence feeds provide a vast amount of information that has to be customised and translated into useful, actionable intelligence. Issues reported include the expense of threat intelligence and there being no specifics for the energy sector or critical infrastructure operators. Actions are being decided and prioritised but without really knowing if the subscribed intelligence sources are sufficient or suitable.

To meet some of these needs, EE-ISAC is currently developing threat intelligence tailored to the energy sector through their Malware Information Sharing Platform (MISP). EE-ISAC aims to enrich the threat intelligence community by giving interesting outlooks on the trends of the threats and attack schemes affecting the energy sector.

#### 6.4.1.6 *Effectiveness of risk assessments*

Standards such as IEC27001 are being implemented. There are concerns over the lack of visibility of risks and an urgent need for a more comprehensive vision on security risks. It was suggested that a catalogue of relevant threat scenarios would aid preparations and risk assessments. Also, some further guidance on the identification of NIS relevant assets would aid risk assessments.

Cybersecurity is a new area of risk so inexperience may be causing inadequate estimations of risk. With many diverse and heterogeneous stakeholders using different approaches that may vary in their effectiveness, are their processes to assess and manage risks effective and sufficient? While guidance is sufficient in regard to standards and methods for Risk Assessment and Management to comply with the NIS Directive, it is important to consider the effectiveness of the varied processes stakeholders are using to assess and manage risks.

In addition, the energy sector faces specific issues that create additional vulnerabilities and risks, such as legacy systems still in operation and complex supply chains. Risk assessments could be justifying cost reduction more than achieving a risk reduction.

#### 6.4.1.7 *Interdependencies & Cooperation*

Guidelines are available on establishing voluntary information exchange on cross border dependencies. Such methods should formally establish dependencies and information exchange for each sector. With variations in local implementations of NIS, it is recommended that standards are followed such as IEC27001/27019. There are also concerns over dependencies on third parties in the supply chain.

Some good cooperation has been established among stakeholders, but it needs to be more proactive and to take action. A formal communication framework among stakeholders is required to facilitate the required cooperation.

Crisis plans are well defined but not well practised with limited testing capabilities. Simulations to test organisational response are still to be performed and the inter-organisation response, eg national response, or cross-country cyber exercises are also not tested. To meet the needs of their members, the EE-ISAC have been moving towards facilitating incident response preparations for the energy sector but without the formal incumbency.

#### *6.4.1.8 Securing Supply Chains*

There are many issues with dependencies on vendors and supply chains, with insufficient and low-quality cybersecurity implementations and products without built-in security.

Operators find themselves working with suppliers without previous experience of security considerations to ensure the products and services supplied help compliance and are adapting to new security demands and requirements.

In particular, SMEs in the supply chain are facing many difficulties to implement cybersecurity controls at both a technical and organisational level. Bigger players in the supply chain seem to have achieved more.

Utilities are all facing similar issues with suppliers. Rather than multiple activities that increase workloads, there needs to be a combined, risk-based approach to centralise the activity, such as a regular committee to exchange audit results.

It is proving to be a huge challenge to achieve trust along the supply chain. It requires a multi-layered approach to secure end-to-end the chain of organisations, devices and their components coming from diverse companies and geographies.

#### *6.4.1.9 Incident Response*

A platform to facilitate incident response for the energy sector is required with the necessary processes designed and implemented. The EE-ISAC has achieved some steps towards this but without the formal incumbency. Also, the national coordination of a response remains unclear.

There are some difficulties with establishing networks for incident response. Networks with key actors have been established, while establishing response from SMEs is work in

progress. It is challenging to find people who understand the OT context for handling incident response.

#### 6.4.1.10 *Human Capacity*

Addressing the skills gap in cybersecurity that companies are experiencing is an urgent priority. There is a lack of specialists and well-trained people, expertise in cybersecurity is very scarce, and particularly in the area of OT. While the need for cybersecurity experience is increasing with digitalisation, energy companies are continually reducing headcount. Also, fixed pay-scales in utilities make it harder to recruit and retain cybersecurity expertise.

There is a need to increase awareness. The focus is currently with CEOs, CIO and CISOs. Awareness needs to broaden now to involve all of management and cooperation from the whole organisation. It is a challenge to establish security policies involving all employees that encourage responsibility, cybersecure behaviours and cyber hygiene.

#### 6.4.1.11 *Continuous Improvement*

Cybersecurity is a cyclical process with ongoing effort required to maintain security against a new and changing environment. Assuring continuous improvement of a cybersecurity solution after initial deployment requires the skills, capability and having the required processes in place.

The energy sector faces specific challenges that create additional vulnerabilities such as legacy systems still being in place. In many cases it is unclear what legacy infrastructure is actually deployed and what its current status is. Resolving such issues is likely to take several years to be fully compliant.

#### 6.4.1.12 *Incentives for investing in security*

Investment is more being driven by potential penalties under NIS and GDPR rather than by incentives. There is uncertainty over investment decisions and cybersecurity costs are hard to sell internally, in terms of proving its value add.

Due to the increasingly large scale of digital components and distributed devices, cybersecurity costs are not affordable by the utility. Also, price controls imposed on utilities make it harder to recover the costs of implementing security while under pressure to keep energy affordable.

#### 6.4.1.13 *Security standards & compliance*

Defining standards and a unified approach to compliance with NIS would ensure its implementation is adequate and consistent. A combined knowledge of the directive and its

implications and requirements would improve consistency. It was suggested to monitor compliance through a gap analysis between corporate frameworks and national requirements.

Due to different local legislation, guidance from ISO 27001 & 27019 is being followed. With national compliance monitoring having some gaps, standards such as IEC62443 are being used as a baseline for OT security.

#### *6.4.1.14 Application of NIS in different countries*

Multi-nationals are finding there are big differences in framework readiness and maturity across different countries. There are inconsistencies in application of the NIS Directive and definition of OES across different countries, however it is still necessary to implement best practise. There is a lack of collaboration across countries, no single point of contact, or harmonisation of different approaches for companies that operate across borders.

#### *6.4.1.15 Public-Private Cooperation in securing the energy sector*

There are potentially many areas for future public-private cooperation to achieve more resilient infrastructures and essential services.

NIS has achieved an important focus on cybersecurity but there needs to be a clearer path to carrying it out, more energy specific or at least critical infrastructure specific guidance.

This survey has given an opportunity to highlight some of the practicalities of implementation and issues the energy sector faces in turning NIS into reality.

### 6.4.2 Public-Private Cooperation in Energy

The NIS Cooperation Group's Energy Workstream, the public authorities responsible for energy cyber security in their countries, requested a platform for discussion with energy operators so an open meeting was arranged between EE-ISAC and Energy Workstream 8 in March 2019. This offered an opportunity to discuss challenges related to the implementation of the NIS Directive in the energy sector, and the chance for both the Competent Authorities (CA) and energy operators, from different member states, to share their experiences with NIS implementations. The feedback from the above survey of energy operators was compiled and presented to the NIS Cooperation Group. From the policy side, the UK's Department for Business, Energy and Industrial Strategy also gave an overview of their implementation of NIS by Competent Authorities in the UK. The feedback given from the energy sector was broader than the remit of Energy Workstream 8 so appropriate

topics were passed on to other workstreams. EE-ISAC later participated in Workstream 3 on incident response, where member states shared experiences with the implementation of centralized incident reporting platforms using templates and methodologies similar to the ones evaluated by EE-ISAC Members during their digital information sharing foundation. The EE-ISAC appreciate the need for bidirectional reporting on threats and trends, the importance of voluntary information sharing and the complexity of implementing a prescriptive framework. Going forward the perspective of the EE-ISAC community is well positioned to support the remit of relevant NIS Workstreams, alongside other sectorial associations, in determining approaches that are really applicable.

Public private partnerships are of central importance to the adequate protection of critical infrastructures [94]. The session between EE-ISAC and the NIS Cooperation Group was noted by ENISA as the first public-private cooperation in energy cybersecurity. In this way EE-ISAC consolidated its presence as a reference point in European critical infrastructure protection. It has since been written into Article 12 of the NIS2 proposal 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” [95].

# 7 Assessing the progress of EE-ISAC

This section provides an analysis of the EE-ISAC situation awareness network and information sharing activity, its contribution to the energy sector, progress and challenges. It includes a self-assessment by the membership and defines future focus areas, to orient energy sector information sharing and analysis within new procedures and regulations, that now enforce information sharing under NIS2 obligations. The author proposes a trusted hub, dedicated to grid participants, to support effective sharing for private infrastructure operators across borders, who require timely actionable threat information to prepare, and respond fast to incidents.

The sharing of cybersecurity knowledge enables better informed organisations to make more effective decisions on how to prepare and respond. The novel solutions proposed during the DEnSeK project established a vision for the developments within EE-ISAC to work towards [88]. Significant progress has since been made in the formation of the EE-ISAC and the establishment of a network of trust. This has fostered a unique environment for information sharing and collaborative opportunities, with the potential to become a significant enabler of improved resilience for the energy sector. The gradual evolution of EE-ISAC and partnerships with other ISACs is forming a joined-up response for the energy sector to face threats together.

Forming an inter-organisation group with a focus and identity creates trust and builds stability. Especially seeing the same faces at EE-ISAC events has established the consistency to build trust and a feeling of shared responsibility. The formation of working groups clarified different roles and issues and invited contributions from different competencies. This has enabled knowledge transfer by bringing different perspectives and experiences and different points of view to the table, learning how different companies are dealing with similar situations [96].

Each face-to-face plenary has included an informal event. These opportunities have built a social glue between members and a sense of community that is fun and exciting. As a result, a gradual building of trust and openness to share evolved, and the confidential information sharing session as a regular slot that was increasingly well contributed to and became a foundational part of the culture of the EE-ISAC. A study of inter-organisational

partnerships solving problems together and transferring best practice has showed 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 [96]. There has been an increasing willingness, especially amongst the established utility members, to bring their latest operational experiences of dealing with security events to the table for sharing and discussion. This demonstrated the qualities of "a security culture with a cybersecurity heartland" [97] that has formed gradually through partnership, mutual interest and sharing common responsibilities.

To demonstrate how EE-ISAC were creating internal and external legitimacy, achieving successful implementation while learning from mistakes, this section presents the outputs from an interactive online plenary during 2020 that was designed to reflect on the Association's mission statement and next steps to undertake in the future, both internally and with the support available from the new Empowering EU-ISACs project team. Section 7.1 below elaborates specific feedback comments from members during this reflection meeting.

In essence, 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 clearly 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 EE-ISAC's progress in Figure 14 shows the emphasis on marketing and developing partnerships that came first for this ISAC. Contrastingly, the analysis and best practice development and platform activity are still developing. The progress of these different aspects of the ISAC were influenced by the leanings of the most active participants. The availability of technical skills to support the ISAC on a voluntary basis was minimal or came in fits and starts around other commitments, when a member saw the possibility for the ISAC and was able to give some extra effort to lead or contribute to a working group.

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 to protect the energy

supply chain and understand 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 real time monitoring of threats and to provide an early warning function. There was even a desire to coordinate 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.

Limited funding and dependency on in-kind contributions exposes a gap in technical leadership of the ISAC. The foundation of trusted Information Sharing has formed well, especially in regular meetings. However the Analysis Centre is in very early stages and would require funding to take further, especially to match the teams of analysts in their partner ISACs in the US and Japan.

## 7.1 Members Reflection

The following questions were posed to members regarding the activities, priorities, and mission of the EE-ISAC and this section summarise their responses:

### 7.1.1 What is the added value of the EE-ISAC to utilities and to other members?

For utilities:

- Having a close and trusted network to rely on during challenging situations
- Collective strength at EU and Sectorial level and towards regulatory and standardization initiatives
- Learn lessons from others (challenges, experiences, projects)

For vendors:

- Network in the European energy industry
- Getting to know the security requirements of utilities

For academia/research:

- Insight on the training and education needed in the industry
- Staying up to date on activities carried out at the European level (Commission, ENISA)
- Cooperation beyond individual organisations by sharing threat intelligence and securing supply chains

For governmental organisations:

- Receiving an overview of the challenges of energy companies across the EU
- Sharing best practices

- Assessing risks in the sector
- Being a trustful party for discussions with national states

### 7.1.2 What are the most important added value of the EE-ISAC to DSOs/utilities as opposed to the other members?

- Information sharing of and analysing the sectorial cyber risks
- Exchange with knowledgeable colleagues in the industry
- Access to applied research problems
- Solid network of trust where opinions and views on several issues are exchanged
- Direct communication and exchange with members
- Academia/research closer to industry needs
- Insight in incidents and their root causes

### 7.1.3 How has EE-ISAC progressed and grown in terms of the learning curve?

The graph below in Figure 14 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 development 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, EE-ISAC's members perceive the growth of 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.

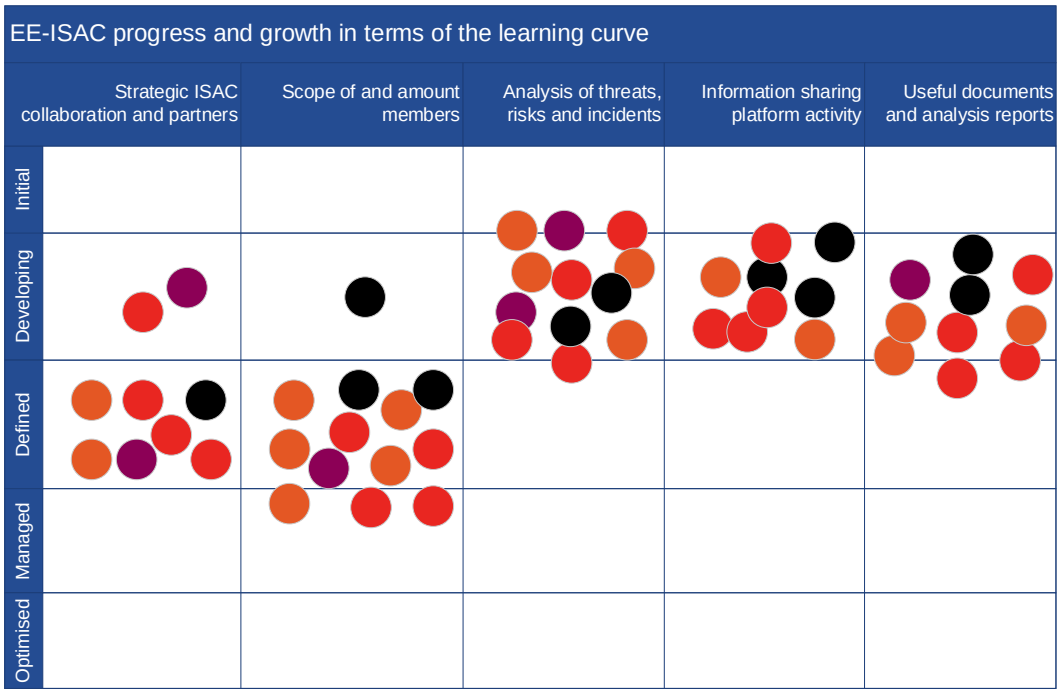


*Figure 14 Progress of EE-ISAC development*

### 7.1.4 Is the mission statement still up to date or does it need to be changed?

As the NIS (with a broad scope, not only focused on energy) and the Network Codes are regulatory frameworks which establish information sharing with different energy stakeholders, DSOs and Transmission System Operators (TSO), a new possible goal to be set for the EE-ISAC in the future is that of establishing itself as the entity responsible for combining some of the NIS and Network Code provisions in order to align them at the EU level. Ahead of the NIS2 proposal, when the previous NIS version did not include a provision for coordination between governmental authorities and the private sector, it was proposed that the EE-ISAC could be the entity playing such a role as intermediary, facilitating public & private cooperation.

In addition, the CERT network structure has the aim of exchanging information for early warning and crisis management for several sectors. So it was also proposed that the EE-ISAC could be a suitable candidate to become the entity responsible for the early warning and crisis management processes for the energy sector.

### 7.1.5 Which objectives do we need to reach to be a more sustainable EE-ISAC organisation?

- Establishing a trusted environment where information can be shared with those responsible for the protection of the European energy supply chain as an element of Critical Infrastructure (CI).
- Preventing attacks on the European energy supply chain elements of critical infrastructure through the development and implementation of “best practices”, “lessons learned” and Incident Response plans.
- Supporting an active community to identify and analyze threats, vulnerabilities and incidents on the unauthorized entrance or manipulation of networks or software supporting CI.
- Enabling public-private cooperation in the field of cyber security related to the energy sector.
- Ensuring membership mutual support via discussion groups, patching information or Q&As.

### 7.1.6 EE-ISAC operates with circle of trust communities or practice spaces. What are the relevant topics today for these groups?

Besides MISP & Threat Intelligence, Incident Analysis & Response and Threat Landscape, the following new topics would be relevant:

- Supply chain dependencies
- Automated and intelligent threat intelligence and analysis (by AI and integration)
- Mapping cross border dependencies
- Education on threats and threat models
- Cross-sector collaboration for threat landscape and intelligence
- SOC/CSIRT Network within EE-ISAC members
- Transform EE-ISAC’s MISP into the official MISP of the energy sector across Europe
- Real-time monitoring of threat-landscape
- Stakeholders group relationship management
- Information sharing on encountered threats (statistics)
- APTs Detection
- Early warning function for the energy sector

### 7.1.7 How can the practice groups be more effective?

- Support with coordination and facilitation of these groups to be more effective.
- Continuous management of practice groups efforts.
- Funding for practice group leadership.
- Progress reports and more integration of non-members.
- Setting roadmaps with clear objectives and responsibilities for each group.
- More feedback from members about the work done in these groups.

### 7.1.8 How can we be the spokesperson for European energy industry for international partners, European Commission (EC) and other associations?

Looking ahead at the next five years, the following ideas could represent the way to move the new strategic roadmap forward:

- Defining a role in EE-ISAC associated to this activity (and possibly a dedicated EU Advocacy group).
- Connecting the EE-ISAC with formal EU structures (CERT EU, ENTSO-E).
- Promoting of EE-ISAC at conferences (done by members).
- Increasing position/influence in stakeholder forums/groups (EDSO, Eurelectric, NIS, Cooperation Groups, Network Code, Editorial teams).
- Establishing defined communication lines to international partners, EC, and other associations.
- Formalising interaction with EC and sustainable funding.
- Defining clearer benefits for the EC and energy sector when acting with EE-ISAC.
- Facilitating anonymous contributions from utilities, to be a combined voice for the energy industry.

To conclude, as in Europe the number of actors involved in this field are increasing, in order to maximise efforts and the impact of EE-ISAC's output from the past five years, it is fundamental to define a new way forward to establish a central role for the Association and create leadership. The EE-ISAC can be a collaborative tool to mitigate risk. How this potential is leveraged to lower the risks together requires innovation and the strengthening of relations with existing stakeholders.

## 7.2 Limitations of the ISAC

EE-ISAC has achieved progress in all five of the key success factors defined at the outset, see Section 6.1.1, however the cybersecurity landscape is more intense now and member needs and requirements have changed. There are also more regulatory pressures to meet and the ISAC role needs defining within this new context. The MISP project has commenced the tailoring of intelligence to the energy sector, partnerships have offered further analysis. To enhance the cybersecurity resilience and preparedness of the energy sector will require more proactive sharing and further progress with analysis of threats, risks and incidents. Section 7.6 proposes several new focus areas for EE-ISAC going forward.

The limitations of a voluntary association have been real, in terms of both funding and time required to sustain the contribution provided by the ISAC. There are limits to how much time and effort each industry member can give to the network. This is in stark contrast to international partners US E-ISAC and JE-ISAC who are government funded with significant teams of analysts. EE-ISAC has participated in consortiums applying for European funding by offering their network of utility members to test, trial and review new cybersecurity solutions and implementations but await a successful application. The ISAC has more recently had to back out of participation in funding calls due to not having the resources to follow through with the time and skill commitment.

The focus areas proposed by this work has prompted EE-ISAC to begin efforts to formalise their role within the new procedures and regulations. There are concerns that regulatory obligations to report incidents leaves the operators with less motivation to also share voluntarily within the ISAC and the focus on national NIS implementations for operators has reduced voluntary effort towards EE-ISAC activities. Similarly, in efforts towards more efficient energy use, a qualitative difference has been shown between voluntary and mandatory energy audits, with voluntary audits presenting a better quality with greater energy saving improvements achieved than the mandatory audits [98]. However, there is also a strong desire to continue sharing between companies if a potential ‘tsunami’ of data from NIS2 incident reporting to authorities slows down information sharing facilitated by national authorities.

The challenge of being a voluntary association with dependency on in-kind contributions has also presented some practical issues due to different identities accessing platforms. For example, an EE-ISAC member hosting the MISP server needed to provide a separate VPN service for EE-ISAC members outside of their organisation to access the platform. This also presented as an issue when members were offered access to partner portals but were entering from different member organisations rather than coming from an EE-ISAC identity.

## 7.3 Accountability

Energy utilities are accountable for providing energy services within the nations in which they operate and for ensuring their infrastructure and services are resilient to cyber-attack. PPPs and ISACs have become an important mechanism to improve governance in cyber security and have been encouraged by governments. They offer an innovative form of governance that makes up for limitations of national governments and inter-state politics by bringing together key actors from private and public sectors towards a common cause. Modern governance structures need to adapt to constant change and be open to new actors. More effective policy implementations require cooperation at all levels to draw on a diverse set of skills and resources at international, regional, national, and local levels [99].

Reliance on such partnerships in other sectors has been challenged due to lacking accountability and democratic legitimacy by having no formal accountability pathway to government or civil society. For a PPP initiative to relate to overall policy goals and ensure it is operating in the public interest, Meadowcroft recommends meta governance by elected bodies. Even though governments may leave some activities to partnerships, they still have a responsibility to ensure those partnerships serve the common good [85].

The EE-ISAC was initially supported by the NCSC in Nederland during its launch and in its first year. It is now member driven and is a legal entity under Belgian authorities. A Terms of Reference (ToR), that each member organisation commits to, defines the rules for information exchange and a confidentiality agreement on the non-disclosure of information that is classified by a Traffic Light Protocol (TLP). Members vote for Board members every two years and the ToR ensures at least 3 out of 5 Board Members come from an energy utility. The ISAC is accountable to its paying members and aims to add value by assisting

members with their own cybersecurity responsibilities. Public involvement is ensured by ENISA being a member of the ISAC with two representatives engaged in ISAC activities.

More recently, to connect the EE-ISAC to policy initiatives, a practice group was formed with an EU Advocacy role. The current goals of this group are to:

- Position the EE-ISAC as the main reference organization for cybersecurity in Europe in the energy sector and critical infrastructures.
- Strengthen the relationship with EU Institutions and key stakeholders.
- Contribute to EC public consultations relevant for the sector.
- Apply for relevant EU- funded opportunities/projects.

With regards the reputation of companies in relation to cybersecurity. It is now widely accepted to take Environmental, Social and Governance (ESG) factors into investment decision making, as a recognised framework for managing business risks. Cybersecurity has grown beyond being an IT issue to becoming an important governance issue and indicator of management competence. Looking after data privacy and customer data links to the Social factor of ESG. Cybersecurity as a Governance factor relates to wider operational loss and increasingly requires recognition and governance of the risks at Board level. As it becomes included as an important G in the ESG framework, EE-ISAC should aim to support the inclusion of cybersecurity in governance processes and be assisting the cyber performance of their members [100].

## 7.4 Future decision support for cybersecurity

The layers of information sharing required within the private sector, the public sector and across PPPs, must consider and support the decision making required at different levels to prepare for and respond to incidents. This refers to strategic, operational and technical perceptions and having cybersecurity capability at each of these levels [101].

The strategic level requires ongoing evaluation of cybersecurity level, with decision processes to ensure adequate resourcing for the required improvements. The strategic perception aims to maintain trust and reputation, by understanding the impact of events on services and users, on the organisation and other actors on the power system. It includes the duty to notify incidents to the relevant authorities. In addition to establishing at least a basic cybersecurity level for energy operators, it requires having crisis management capability in

place for cybersecurity events with national or cross border impact. At the core of information sharing with industry networks and with national authorities sits the essential need for proactive protection.

The operational level requires the ability to keep functioning, to maintain business processes and recover from events. It includes establishing functional collaborative networks to assist preparations and enable faster recovery during significant incidents, including support from supply networks, public authorities, NCSCs and sectoral ISACs.

The technical perspective includes the ability to monitor through a SOC capability to detect and manage events, and the ability to analyse events and classify their severity. This indicates the relevant parties to inform, internally and externally, including compliance with incident reporting requirements where energy supply services are impacted.

The predominant emphasis on utilising knowledge-based information to defend against known attacks with intrusion detection, vulnerability scanning, attack signatures etc. needs to broaden into unknowns. With uncertainties over how threats will evolve, a more proactive and adaptive approach is required to deal with unknown threats to operational environments and to detect new attacks at an earlier stage. Building capability to face new scenarios requires continuous effort to adjust to emerging threat intelligence as attack strategies change. It is important to have a continuous process in place for building threat awareness and minimise vulnerabilities to the evolving state of attacks. Trust networks such as ISACs have the potential to provide an information hub, tailoring information for their sector. Use of external threat intelligence should also be combined with some internal threat intelligence i.e. by monitoring of OT events, communications on control network, and information from endpoints. Mostly through passive monitoring to minimize impact on performance of OT devices and with some active polling of devices. Anomaly detection is also necessary to detect earlier stages of a new attack by seeing deviations from normal activity. This could assist in providing the early warning notification requirements proposed by the Network Code on cybersecurity and incorporated into NIS2 [102].

The trust circles and collaborations across public and private actors that are being encouraged and reinforced by the NIS2 [95] obligations must build capability at each of these perception levels with the sharing of useful and actionable information.

## 7.5 NIS2 & Cross-border relations

The main responsibility for cybersecurity governance under the NIS Directive remains at a national level. Different implementations resulted in a lack of coherence and consistency between member states, some states lacking a cybersecurity strategy, others setting their own cybersecurity priorities. Private companies operating across borders were experiencing different approaches from national authorities. Following a review of NIS in 2020, the NIS2 proposal aims for a more consistent level of cybersecurity across member states. A key objective of NIS2 is to promote effective information sharing, as described in Table *17*, and introduce additional cross border responsibilities for Member states, with a more significant role for ENISA to coordinate response to major events.

The EU have been encouraging participation in ISACs through their funding mechanisms. NIS2 is "not simply disciplining the exchange of information at the institutional level between the national competent authorities" [95]. Participation in information sharing between companies is now included in entities' notification responsibilities to CAs under NIS2, citing EE-ISAC as an example of "already existing capability and well-established frameworks" [95].

This definition of information sharing mechanisms implies a separate sharing channel between companies, within trusted communities or ISACs, to the sharing channel between national authorities. Nation states can be concerned about sharing too much operational information or affecting the economic interests of their companies [103]. In this situation energy operators have expressed frustrations over inadequate cooperation across borders between member states and EE-ISAC are requesting some involvement in the process of information exchange.

| **NIS2 information sharing mechanisms** [95] | |
|---|---|
| Between companies | Article 26 requires companies to exchange relevant cybersecurity information among themselves within trusted communities, Companies are required to notify Competent Authorities (CA) of their participation in such information sharing arrangements. Members states will adopt policy procedures and appropriate tools to support this sharing activity (Article 5) and will define the extent of their involvement in these communities. |

| | |
|---|---|
| Between companies and 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 are obliged to provide assistance with mitigations for the reported incident or threat. Article 27 also invites voluntary reporting from companies outside of the scope of NIS. Article 6 requires national Computer Security Incident Response Teams (CSIRT) to coordinate vulnerability disclosures. |
| Between national authorities | Article 11 requires cooperation between competent authorities, CSIRTs and SPOCs within each member state, in providing information on risks threats and incidents. |
| Between member states | The National Competent Authorities are brought together under the NIS Cooperation Group. Cross border impact of reported incidents and near misses is assessed by the national authority and information passed to other member states and ENISA as required. SPOCS provide monthly incident summary reports to ENISA.<br>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. The NIS Cooperation Group, CSIRT network, and European Cyber Crises Liaison Organisation Network (CyCLONe) will provide opportunities for cooperation between Member States. Mutual assistance between member states is also introduced through a peer review mechanism. |

Table 17 NIS2 information sharing mechanisms

With a formal structure for cooperation among members states at an EU level now defined by NIS2. How will this translate to practical support for private infrastructure operation across borders, who require timely actionable threat information to prepare, and a fast response to incidents? Also, how can the cooperation foundations already established in ISACs be incorporated into this situation most effectively? The cross-country exchange of information, from operators to national authorities, back to other national authorities has not been running smoothly. Notification obligations under NIS have required energy operators to share information to their authorities but there is often a feeling that assistance

from government agencies has not been reciprocal [104]. As authorities are receiving notification of incidents from both essential and important entities, attention needs to be on minimising the impact of incidents. 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 rapid closure of vulnerabilities. A two-way process is most advisable, by requesting national authorities to also report to operators or sectoral ISACs on incidents, rather than only the company obligation to report to authorities. The ISACs are in a position to enrich the information, making it sector specific, to provide more actionable information to their utility members. OES across Europe are also encouraged to report "near misses" and disruptions threatening their IT or OT critical infrastructures to their supervisory authority. It is also important that the national competent authorities inform other operators in Europe of such attempts of attack, i.e. indicators of compromise, so they can promptly verify whether they are also susceptible and subject to such risks, and initiate suitable countermeasures. Additionally, ISACs play a fundamental role to analyse, at the international level, potential weaknesses and early indicators of threats that could be meaningful as ex-post incident analysis and reporting.

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" [95]. As the CSIRT Network exchanges relevant information on cyber threats and incidents occurring in Europe, and inform 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 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 their obligations to share between companies, operators expect to continue direct exchanges among TSOs and DSOs to manage energy sector responsibilities, while the national competent authorities govern the process with their policy for sharing, rather than being an integral part of the actual information shared.

### 7.5.1 Network Code on Cybersecurity

A collaboration of European TSOs and DSOs, involving ENTSOE and EDSO, have proposed a Network Code on Cybersecurity which 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 grid participants of the Continental Synchronous area spanning 28 countries, operated by ENTSOE. Participants in this synchronous area may impact their neighbours during a cybersecurity event if the consequences affect power flows on the system. This activity to develop a Network Code for cybersecurity sits within the strategic level described in Section 7.4. It is an opportunity to create a translation of NIS for the energy sector particularly with regard to cross border impact. ENTSOE, EDSO and national CAs will create a list of cybersecurity principles that electricity entities must meet.

There was concern and criticism that the Network Code seemed to be overlapping with or duplicating NIS. This is a prime example of the challenges in PPPs when public and private participants come from a different point of reference The information sharing mechanisms proposed by Government in NIS2 uses national borders as its framework whereas the actual operational and technical boundaries differ. The operational boundaries of energy companies can be within a member state or operating across borders for larger organisations. The technical boundaries correspond to the synchronous AC grid area, that is electrically tied at the same frequency, where power supply and demand is balanced in real time.

The Network Code is defining the operational and technical cybersecurity requirements alongside the national expectations laid down by NIS2. By involving NCAs 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.

Due to the CSIRT network established by NIS being likely to prioritise dissemination across sectors nationally first before attending to international dissemination, during the NCCS drafting process shortcuts were requested, see Figure 15, for information flows so that dissemination to grid participants can happen direct from a CSIRT in another state where the information originated. Rapid sharing is important to minimise cascading effects in a connected grid.

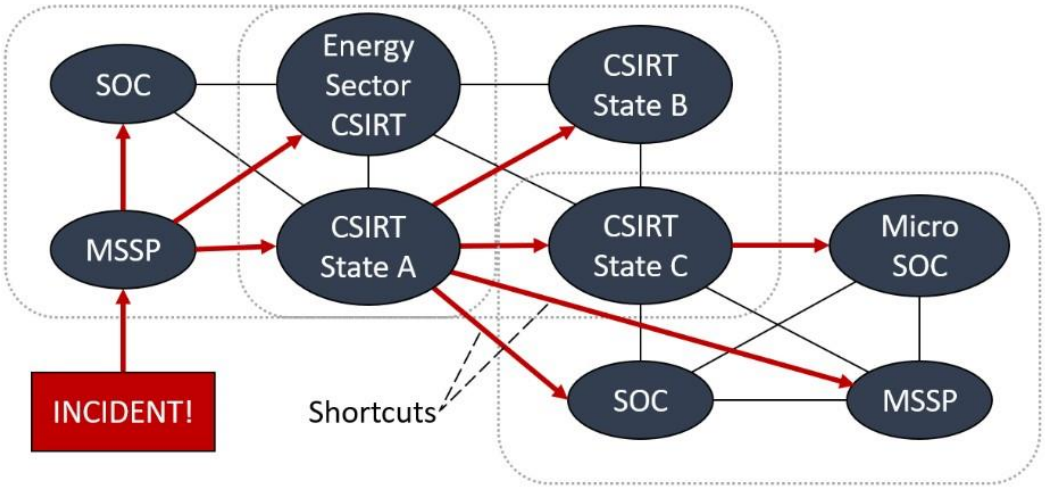


*Figure 15 Proposing shortcuts for more direct information sharing*

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 [105]. Providing a combined view to such entities in an anonymised and secure manner could be a future role for EE-ISAC in collaboration with ENTSOE and EDSO. 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. They must be able to alert other electricity entities and respond rapidly themselves when alerted. The Network Code recommends grid entities to establish a SOC or to access SOC capabilities through a Managed Security Service Provider (MSSP) to ensure incident response capability at the entity level, unless the CSIRT at national level is engaged to handle incidents. [106] This voluntary sharing among electricity entities in the synchronous grid area is described at Figure *7* in Section 4.2.1.and offers a synthesis of regulator and operator suggestions during the Network Code drafting process.

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. It is proposed 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 [107].

Further to the strategic direction provided by the Network Code, EE-ISAC can assist at the operational and technical levels, described in Section 7.4, interpreting events together. The trusted network in EE-ISAC provides a network of support for utilities, that includes researchers and solution providers. EE-ISAC activities should contribute to assisting energy sector companies with meeting their obligations under NIS2 and the Network Code on Cybersecurity. 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.

## 7.6 Future focus areas for EE-ISAC

The EE-ISAC network of trust can be a collaborative tool to mitigate risk. How this potential is leveraged to lower the risks requires innovation and the strengthening of relations with existing stakeholders. NIS2 now obliges companies to join an ISAC and report their participation to their national authority. It is therefore important that ISAC activities steer towards assisting energy sector companies with the goals of NIS2. The participation of companies in an ISAC, required by Article 26, would benefit from being somewhat defined and scoped. The original key success factors defined in Section 6.1.1 have now mostly been achieved by EE-ISAC. This section proposes five key focus areas for EE-ISAC, to steer future progress in energy sector information sharing and analysis initiatives.

1. **Contribute to achieving a common level of cybersecurity among participants**

- Assisting members to achieve their objectives under NIS2 and the Network Code on Cybersecurity, for example through developing best practices together.
- Connect EE-ISAC activities to EU structures where energy specific assistance is relevant. For example, the CERT network structure has the aim of exchanging information for early warning and crisis management for several sectors. Through further definition of processes, the EE-ISAC exchanges could support early warning and crisis management for the energy sector. EE-ISAC should continue to offer a combined voice for the energy sector to provide anonymised feedback to the

regulation and policy arena as required. In particular, investigating with NIS Cooperation group and CSIRT network the utilisation of ISACs to provide sector specific actionable and usable information to utilities from the incident information reported to authorities i.e. the feasibility of a two-way reporting process proposed in Section 7.5.

- Develop a central cybersecurity information hub and communications channel for the energy sector, facilitating the sharing of best practices and disseminating mitigation strategies.
- EE-ISAC should continue to offer a combined voice for the energy sector to provide anonymised feedback, where necessary, to the regulation and policy arena. Continue to provide energy sector specific feedback into NIS2 and Network Code developments and ENISA activities.

**2. Spread cybersecurity capability improvements and share knowledge**

It will be important to gather the most appropriate stakeholders to the table to complement NIS2 and better support cross border NCCS activities. This may require some sharing and exchange of best practices beyond the membership as well as attracting the most relevant players into the association:

- Sharing relevant experience with new entities, as the risk picture changes and new entities are identified as essential or important under NIS2 or the Network Code.
- Information sharing with new countries entering the continental synchronous area.

**3. Analysis Centre**

As Section 7 indicated, the foundation of trusted Information Sharing has formed well, whereas the Analysis Centre would benefit from further development. A good foundation of cooperation has begun through the MISP project, it is now important to facilitate more proactive sharing and to progress the analysis of threats, risks, and incidents. The association has fostered a culture of trusted sharing particularly in the face-to-face meetings. This could be progressed to take actions to help each other such as with early indication and formulating guidance from joint experience.

**Threat Analysis.** Provide more actionable threat intelligence than what utilities currently have access to. Tailoring threat intelligence to the energy sector, progress the MISP project as a platform for the wider energy sector. Progress towards real-time monitoring and analysis of threats and to provide an early warning function. Utilise collaborations with

international ISACs and cross-sector ISACs to improve threat intelligence. Quickly disseminate new information to assist utility preparedness eg IoC analysis or malware reverse engineering etc.

**Strategic Risk Analysis & Consequences**. Contribute to understanding a more holistic picture of risks with continuous risk assessments. Provide sector knowledge on the potential impact of technology changes and system differences. For example, consider 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 small DSOs. Offer sector experience to attend to potential gaps in NIS implementation or Network Code application, reviewing the process for applying the Network Code to different entities, for example where the potential impact on the system rather than size of entity or customer base may be more relevant.

**Tactical Incident Analysis & Response**. Explore the potential for a Security Operations Centre (SOC) network among EE-ISAC members for the energy sector. Particularly in light of the Network Code requiring grid entities to have access to SOC capabilities. Share learning from cybersecurity events. Ensure best practices, lessons learned, and post incident recommendations are disseminated appropriately.

**4. Supply Chains**

Facilitate progress with protecting the energy supply chain and understanding supply chain dependencies. Foster close understanding and alignment with vendors and solution providers in the EE-ISAC membership, communicating the common cybersecurity needs and requirements of energy utilities. Engage with interdependent sectors, especially telecoms sector to ensure cybersecurity across end-to-end solutions.

5. **Performance assessment**

Regularly assess the performance of EE-ISAC in terms of its contribution to operational, regulatory & business aspects of cybersecurity. Look for evidence that EE-ISAC has assisted cybersecurity improvements across the whole energy system and synchronous area, to achieve regulatory requirements and assist businesses to improve their cyber performance. Carry out regular stakeholder reviews paying particular attention to the below to keep on track with the goals of the ISAC.

- Regular assessment of the contribution of the ISAC community towards improving the cybersecurity level of members as required by NIS2 and the Network Code.
- Check if EE-ISAC activities have assisted member companies to make improvements in their cyber performance. With cybersecurity becoming an increasingly important governance issue and an indicator of management competence, assess if the EE-ISAC approach is supporting the Governance aspect of their members' ESG performance.
- Assess the level of engagement and impact beyond the membership that assists overall improvement of cybersecurity for the Continental Synchronous area as a whole.

Emphasising these focus areas will also indicate the performance improvements intended by NIS2, outlined in Annex 7 - 1.4.4 in [95]. In particular, NIS2 is looking for increased transparency among operators when managing cyber incidents. A culture of managing cyber threats that considers the whole infrastructure system, rather than of competitive division and confidentiality. Passing of information among authorities needs to be reflected in actual improvement in cybersecurity level on the ground.

Maintaining the ISAC with an appropriate balance of members and ensuring it is adequately funded and resourced to carry out the above is crucial. Continuous management of EE-ISAC practice groups, instead of the current ad-hoc contributions from willing members, is paramount to guide efforts with road maps towards achieving the key focus areas and regular progress reporting. Resolving these issues raised in Section 7.1.7 to increase the effectiveness of the practice groups is central to the success of EE-ISAC in achieving a valued contribution to the energy sector and a model for other sectoral ISACs.

## 7.7 Interdependent Assurance of Energy Systems

An essential aspect of cybersecurity governance is the co-operation between interdependent organisations. The regulatory activity underpinning the cybersecurity of our essential services is dynamic, with multiple actors participating. It requires coordination across a distributed accountability and effective communication across actors to improve their capacity to make more informed decisions while protecting our infrastructure and responding to events [108].

Cybersecurity is too complex an issue for organisations to handle alone. The importance of collaboration is emphasised by many, and examples exist beyond the EE-ISAC, such as the UK's Cyber Security Information Sharing Partnership (CiSP) enabling industry and government to share threat information [109]. The Cybersecurity and Infrastructure Security Agency (CISA) in the US have an information sharing program across all critical infrastructure sectors that supports collaboration through trusted public-private partnerships [110]. Europol have provided a website for public and private entities to share, this includes providing access to decryption tools for assistance with ransomware recovery [111].

This research has provided an example of the progress, challenges and effort that have built a trusted network and deepened cooperation among energy sector participants both within Europe and globally. Pooling of information from different sources is now possible, some partners are sharing more than ever before. However, it is essential that sharing happens in a timely manner and that it is tailored into actionable information for it to be useful and effective. The shared responsibility across different organisations in responding to attacks needs to be better rehearsed with regular exercises. Future information sharing mechanisms, forming under the new NIS2 obligations, need to build on and improve what is already established, rather than create new structures for sharing. Skills and resources in cybersecurity are limited so it becomes essential that efforts towards regulatory compliance also result in improvements in cybersecurity. Most importantly, efficient and effective collaborations are crucial due to the fast responses that are required in a fast-changing sector. The inter-organisational cooperation necessary to thwart cyber-attacks requires the translation of NIS2 cooperation mechanisms into a cybersecurity strategy that is co-owned within partnership arrangements, and instigates combined action from partner members [97].

# 8 Interorganisational Cooperation in Securing Supply-Chains to Critical Infrastructure

This chapter provides a study of interorganisational cooperation within the context of securing supply chains to critical infrastructure. It includes a cross-industry comparison of the UK's implementation of the NIS Directive, that placed the responsibility for supply chain cybersecurity onto Operators of Essential Services (OES), prior to the inclusion of supply chain assurance in the NIS2 proposal by the EC. Recommendations are made from this experience that enhance previous supply chain guidance provided by the NCSC.

The transposition of the EU Directive on Network and Information Security (NIS) by EU Member States involved assigning a set of responsibilities to operators, regulators and policy makers within a National Cybersecurity Strategy, in order to improve cybersecurity levels across critical infrastructures. This research investigates the perspectives and experiences of organisations affected by the NIS Directive focussing on three different sectors (Energy, Water & Aviation). This research evaluates the response of different actors to NIS interventions and their challenges in meeting their assigned responsibilities, in particular their ability to oversee supply chain cybersecurity. It proposes further support for partnerships and cooperation across organisations to increase the effectiveness of NIS implementation. Based on results from semi-structured interviews and observations of industry working groups, an approach to supply chain oversight to achieve a balance between control and cooperation is recommended, to improve cybersecurity within industry sectors and across critical national infrastructures. The focus in this Section 8 was to work mainly with UK stakeholders however the recommendations will have a more general application now that NIS2 proposes all member states include supply chain responsibilities in their NIS expectations. The recommendations also apply beyond those countries directly affected by the NIS Directive. This research is published in the following reference and was presented to the UK Cabinet Office & Lead Government departments:

Tania Wallis, Chris Johnson, and Mohamed Khamis. "Interorganizational cooperation in supply chain cybersecurity: a cross-industry study of the effectiveness of the UK implementation of the NIS Directive." Information and Security: An International Journal 48, no. 1 (2021): 36-68. doi.org/10.11610/isij.4812

## 8.1 Regulation of Critical Infrastructure

The EU Directive on Security of Network and Information Systems (NIS Directive) was introduced in 2016 to raise the cybersecurity level of Critical National Infrastructures (CNI) across EU Member States [112]. A reform of the Directive was proposed by the European Commission in December 2020 known as NIS2.0 [95]. The original objectives of the NIS Directive are still considered as very relevant:

- To increase the capabilities of Member States in mitigating cybersecurity risks and handling incidents.
- To improve the level of cooperation amongst Member States in cybersecurity and the protection of essential services.
- To promote a culture of cybersecurity across all sectors vital for our economy and society.

It applies to industries providing essential services to society such as Energy, Water, Transport, Health and Finance. The interpretation of which companies fall within scope across these industries is a matter for individual member states. The NIS Directive places a responsibility on national Governments to secure their essential services. The transposition of the NIS Directive by each national Government decides the services considered essential for their nation and applies the regulation to the public or private operators of those services.

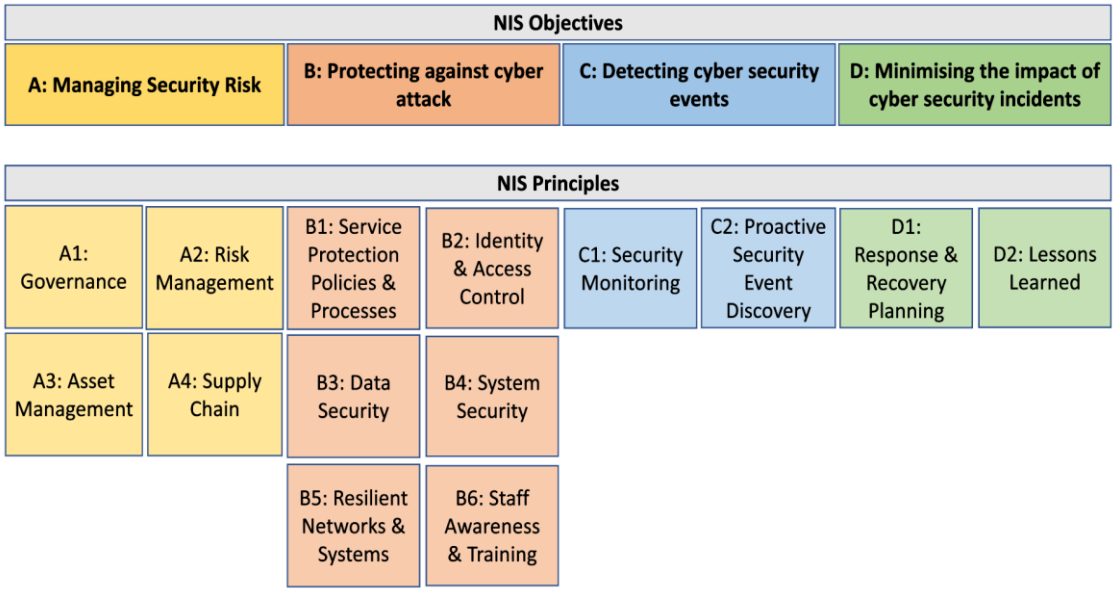


*Figure 16 NIS Objectives & Principle* [113]

It was transposed into UK law in 2018 as the NIS Regulations. These regulations are still in place following the UK's departure from the European Union and will be reviewed by the UK Government during 2021.The UK National Cyber Security Centre (NCSC) produced a collection of guidance for the implementation of the UK NIS Regulations. Figure 16 outlines the principles and objectives that are defined in the NIS Guidance Collection [113]. This paper evaluates the response of different actors to these NIS Objectives & Principles and their challenges in meeting this intervention.

The original NIS principles are further outlined in Table 18; this provides an overview of what is expected of each operator of essential services as defined under the NIS Regulations.

| | |
|---|---|
| **Objective A** | Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to essential services. |
| **Objective B** | Proportionate security measures in place to protect essential services and systems from cyber-attack. Includes: identity and access control, data and service security, information protection policies and processes, protective technology and staff awareness and training. |
| **Objective C** | Capabilities to ensure security defences remain effective and to detect cybersecurity events affecting, or with the potential to affect, essential services. Includes security monitoring and anomaly detection. |
| **Objective D** | Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary. Includes response and recovery plans. |

Table 18 NIS Principles [114]

The NIS Directive introduced key roles and responsibilities as listed in Table 19.

| Role | Responsibility |
|---|---|
| **Operators of Essential Services (OES)** | Implementing NIS Principles.<br>Required to report incidents affecting essential services to the Competent Authority. |
| **Competent Authorities (CA)** | Produce guidance & cybersecurity assurance goals.<br>Audit and assess the cybersecurity levels achieved by OES.<br>Enforce compliance where necessary. |

| | |
|---|---|
| **Computer Security Incident Response Teams (CSIRT)** | Provide technical expertise.<br>Assistance with cybersecurity incidents. |
| **Single Point of Contact (SPOC)** | International co-operation and engagement with EU partners.<br>Participation in the NIS Cooperation Group. |

Table 19 Roles & Responsibilities introduced by the NIS Directive[113]

The NIS Directive expects national Governments to have a National Cybersecurity Strategy with the goal of improving the cybersecurity level of their critical infrastructure and securing the services essential to their society. Figure 17 shows how the UK's implementation of this high-level strategy engaged organisations and activities across the public and private sector and demonstrates the full extent of the supply chain being positioned within OES responsibilities. This supply chain includes the hardware, software and systems being used by operators to provide their essential services such as water or electricity supply or transport services. It can include systems integrators who are configuring bespoke designs; providers carrying out maintenance for an operational facility or support services for IT or Operational Technology (OT). The supply chain could also include consultants providing relevant expertise to an OES. It is up to the OES to decide what is in scope of the NIS Regulation by defining the critical assets and suppliers that their essential service is dependent upon.

The UK National Cyber Security Centre (NCSC) provides overall guidance by producing indicators of good practice that contribute to the outcomes expected by the NIS principles and objectives [114]. The sectoral Competent Authority (CA) provides sector specific guidelines and a profile to be achieved that their assessments and audits are based on. In most cases, the nominated CA was the regulator in charge of existing safety oversight. Examples of organisations assigned the role of CA under NIS include the Civil Aviation Authority (CAA), Health & Safety Executive (HSE), and the Drinking Water Inspectorate (DWI). There is a reliance on OES to relate this to their specific operational context by defining the assets in scope of NIS that their essential service depends upon, assessing their current achievement against the provided Cyber Assessment Framework [114] and creating performance improvement plans that are overseen by the sectoral CA. While this process displayed in Figure 17 implies a passing of responsibility from the strategic level down to

achievement of the goals of the NIS Regulations, this research demonstrates that collaborations and regular interactions are required between the private and public organisations involved to manage progress and provide assistance.

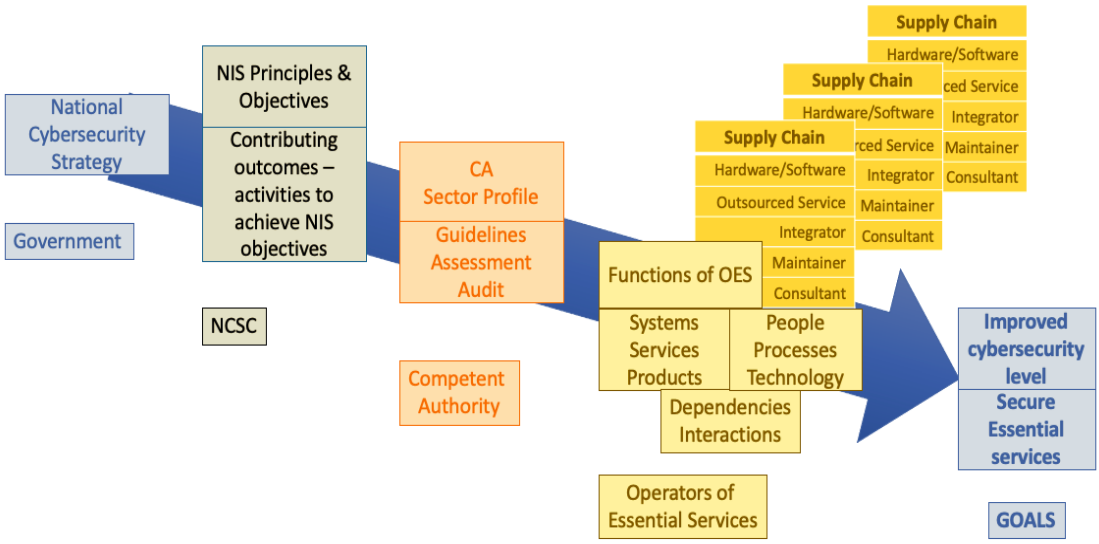


*Figure 17 Implementing the National Cybersecurity Strategy for Critical Infrastructure*

## 8.2 Managing Supply Chain Risks

The increasing digitalisation of CNI together with a need for more distributed forms of control, for instance as a consequence of the pandemic, has increased the need for more enhanced supply chain assurance. With many distributed devices and interactions over a mix of infrastructures, establishing a common level of mutual trust and security across different administration boundaries becomes increasingly important. Reliance on multiple vendors including open-source providers requires a closer understanding of the varying levels of their security so that the context of operational dependencies can inform ongoing improvements. Cyber criminals look for the weakest link where there are fewer protections in place because a single compromise in the supply chain can enable access to multiple organisations. A significant proportion of attacks are targeting beyond one organisation and intending to achieve access to other organisations along their supply chain [115]. Increasingly the vendors and suppliers used extend across national borders raising significant concerns about national security and “digital sovereignty”.

The NIS regulations do not directly apply to the supply chain. Instead, there is a pass down of responsibility where operators need support from their vendors to achieve adequate cybersecurity and reduce risks to their infrastructure. NIS Objective A and principle 4 in the Cyber Assessment Framework requires some oversight of OES supply chains. Table 20 shows some of the expected outcomes to fully achieve this supply chain principle. It requires operators to have a deep and broad understanding of their supply chain risks beyond Tier 1 suppliers and to have clearly defined supplier responsibilities as well as achieve a mutual commitment from suppliers to resolving incidents [116].

| **Expected outcomes to fully achieve NIS Principle on Supply Chains** |
|---|
| Deep understanding of supply chain, including sub-contractors and wider risks, to inform risk assessment and procurement processes. |
| Consider risks to essential functions arising from supply chain subversion by capable and well-resources attackers. |
| Information shared with suppliers, that is essential to operation, is appropriately protected from sophisticated attacks. |
| Security requirements of suppliers are mutually understood and laid in contracts, with a clear and documented shared-responsibility model. |
| All network connections and data sharing with third parties is managed effectively and proportionately. |
| Incident management processes include mutual support with suppliers for the resolution of incidents. |

Table 20 Achieving NIS Principle A4a Supply Chain

This research, on examining the process of implementing the NIS Directive, highlights that OES, as individual organisations, are not in a position to fully secure their infrastructure and services without reaching out in collaboration with other organisations to develop sector approaches and to influence improvements in their supply chains. This creates a potential role for the CAs and wider government agencies in supporting collaborative approaches to supply chain assurance across national industries. There are tensions where this might be interpreted as undue interference in market forces; for instance, if a government agency forced OES to procure key components from an approved supplier list.

## 8.3 Supply Chain compromises

Recent supply chain attacks demonstrate that suppliers are a potential attack route into multiple operators. By compromising one vendor an attacker could achieve access to all the

vendor's customers. Operators can also be caught in the crossfire of attacks targeted elsewhere due to sharing common vulnerabilities. The inability of suppliers to maintain adequate security over the long lifespan that equipment is used in cyber-physical systems exacerbates the situation. There can be several steps to an attack, once access is achieved, the attacker could move laterally within the network and reach more critical assets, such as operational technologies that control critical infrastructure. Layers of security, including segmentation of networks, are essential to minimise the impact of incidents. Urciuoli presents examples of supply chain threats to emphasise the importance of protecting the supply chain information layer [117]. Pandey and Singh describe a range of methods of attacking supply chain systems, from pre-installed malware on manufacturer components, to Denial of Service (DoS) attacks compromising availability of resources, direct attacks to damage and destroy services and, in particular, the ease of initial attacks against a third-party enabling access to their ultimate target [118].

A global supply chain survey by BlueVoyant reported that 80% of participants had experienced a third-party breach during the past year and 77% have limited visibility of their supply chain, with only 2% managing to monitor their vendors in real time or daily. The energy system is becoming more distributed with an increasing reliance on third parties. Distributed DoS is a key concern for the energy sector as well as third-party compromise of their SCADA systems [119].

The continued obligation on OES to maintain their essential services has resulted in them being ideal targets for disruptive attacks such as ransomware. Such attacks block access to important data until a ransom is paid and create an urgency to pay with threats to publish the stolen private and confidential information within a short timeframe. Several energy firms experienced ransomware attacks in 2020 such as the Ragnar Locker ransomware impacting Portugal's energy operator EDP, which targeted software used by their Managed Service Providers [120]. The Netwalker ransomware affected K Electric in Pakistan and multinational energy company Enel [121].

Attacks in the water sector have resulted in a diverse set of impacts such as polluting water ways, data breaches and theft of irrigation water [122]. The water sector is dependent on the supply chain for essential chemicals for water treatment and therefore could be

impacted by unauthorised intrusion into the ordering systems of their suppliers. A recent attack on a water treatment facility in Florida attempted to manipulate chemical levels in the water by adjusting set points. This attack emphasised the importance of maintaining integrity of system configurations, managing remote access to operational facilities as well as the human aspect, the anomaly in operational settings was discovered and corrected by a human operator [123].

The aviation sector has experienced DoS attacks on air traffic communication channels and malware being introduced by sub-contractors into air traffic management systems. Airports already give much attention to physical security and require equivalent attention to cybersecurity, such as controlling digital access to their operational equipment [124]. Also, recovering safely from incidents is essential and requires close coordination with IT service providers to ensure safe operations are preserved during incident response and recovery [125].

Aviation companies, along with other critical sectors, were alerted to consider their supply chains during the SolarWinds cyber-attack in 2020, which enabled the theft of FireEye's 'red team' tools that are used to test client defences by emulating adversaries. The attack also targeted the US Federal Government & US Military and was achieved through a malicious software update by deploying malware as an update from SolarWinds' own servers. It was digitally signed by a valid digital certificate bearing their name. When customers updated the software, a backdoor was installed into their server. Its impact goes far beyond the original targets, after being unknowingly installed by IT administrators across 18,000 or more organisations. It has also left uncertainties due to the exposure of backdoors enabling additional exploits before discovery and patching was carried out [126] [127] [128].

Microsoft exchange servers have recently been attacked globally by utilising four different vulnerabilities to gain high privileged access to the servers, prior to authentication and without valid credentials. Attackers could use this as a stepping-stone to reach other parts of the breached network, giving the opportunity for further exploits such as data theft or installation of malware. This attack demonstrates the importance of having an up-to-date asset inventory to find the affected systems quickly and take remedial actions. There can be a time lag before patching is possible, especially in operational environments, where it is

important to first assess if the patch would have a negative impact on system operation [129].

The theft of customer records from credit reporting agency Equifax in 2017 was achieved due to an open source software vulnerability. The lessons from the Equifax incident showed that implementation and management of security is just as important as having security procedures in place. Procedures were in place but the software vulnerability had not been patched. There was no network segmentation configured, attackers were able to go from machine to machine. Role based access control was also not set up, the system gave access to all the content once compromised. Anomaly detection for unusual behaviour was also not installed, thousands of database queries in rapid sequence was not alerted. Despite Equifax having a high spend on security, the actual implementation of it was inadequate[130]. Breaches related to open source components have reduced since the Equifax incident but are still occuring often. In Sonatype's survey of software developers 20% experienced a breach in 2020 that was tied to an open source component [131]. Attackers are also not limited to exploiting the existing vulnerabilities within open source components. Malicious actors now proactively target open source projects by newly infecting software components to distribute malware [132].

## 8.4 Related Work

Sobb & Turnbull point out the need for additional research on evaluating the risks introduced from supply chains into operational environments and how to securely integrate supply chain technologies into such contexts [133].

Other research methods have provided supply chain attack surface diagrams to assist with identifying gaps in current practices [134]; have modelled threat scenarios and potential attacks coming from a supply chain perspective [135]; and adapted attack graph generation methods to a dynamic supply chain environment to assist administrators with protecting assets [136].

The international standard IEC62443 describes various aspects of industrial cybersecurity, including IEC62443-2-4 which specifies the security capabilities required of providers to industrial control systems[137]. ENISA provide good practices for cybersecurity across the supply chain for Internet of Things (IoT) [138].

Previous research has recognised that a single entity alone does not possess the full capability to respond to cyber threats without some level of cooperation with other entities. Polischuk recommends to focus and multiply the necessary capability through a flexible and adaptive national security system with effective communication between the elements of this system [139].

Penchev proposes to establish focus groups under an umbrella organisation for the necessary cooperation between civilian and military organisations in cybersecurity[140]. Other work exemplifies building an integrated collaborative information environment for more effective working across organisations during crisis management and to support decision making at different levels of Government[141]. This research provides a synthesis of this necessity for interorganisational cooperation in cybersecurity with other related works on the performance and resilience of supply chains, from supply chain management literature that are outlined in Section 8.6.

This study evaluates the experiences of implementing the NIS Directive across the public and private sector. It presents recommendations on supplier assurance and offers a timely contribution as the EU proposes to broaden the application of the NIS Directive and bring supply chains under the NIS umbrella. NIS regulated entities who deliver essential services in the EU will be required to "assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures." [95]

## 8.5 Supply Chain Responsibility

Responsibility for cyber security seems to be spread across extensive supply chains. While work can be outsourced, risk cannot, and the impact of a security failure cannot be outsourced either. With the issue of decentralised accountability across supply chains, it remains the operators' responsibility to ensure suppliers have appropriate security in place.
In reality, the responsibility for cyber security that is ensured by contracts with vendors can often sit across many departments with various different supplier relationships. Carrying out audits could uncover cyber security practices of 3$^{rd}$ parties rather than assuming contract agreements have it covered. Although suppliers have received multiple assessments from all their customers, all slightly different, which is a considerable overhead to respond to. While

cyber security can be approached by separating the system into zones and protecting access to them, there is still a reliance on suppliers inside each zone. Some of the design and management of zones is outsourced and components from 3rd parties exist in each zone. These supplier relationships across the whole system lifecycle need to be considered to build a picture of the various dependencies. The dependencies can also have layers to them to include subcontractors engaged by suppliers. Engaging in cyber secure interactions and establishing security procedures with suppliers would encourage the ongoing behaviours required of Smart Grid organisations and suppliers.

The industry interviews carried out uncovered that responsibility for cybersecurity can become blurred when there are multiple actors, components and systems involved. There is much work in progress to ensure responsibilities are defined and understood. This issue is explored here in the light of related works.

The IEC standard 62443 states that all actors have a shared responsibility for Industrial Control System (ICS) cybersecurity including suppliers, integrators and asset owners: through secure development by suppliers; secure deployment by integrators; while asset owners configure, operate and maintain security over time [142]. Accountability for cybersecurity remains with the operator asset owner, despite reliance on products and services from the supply chain. The operator retains responsibility for decisions made and the effectiveness of their security even if outsourcing for assessment or advice or to a cybersecurity solutions provider [143]. Where responsibility is delegated to a supplier, it is important the accountability for the effectiveness of this approach is retained within the operator. Management of the delegated responsibilities should include a requirement that cybersecurity responsibility sits at a senior level within the supplier organisation to ensure senior management support for their security responsibilities [144].

OES identify the critical assets that their essential service depends upon. This provides a scope that the NIS Regulations can be applied to and becomes the focus for assessment and improvements [145]. However, this scope could broaden when remote maintenance is carried out or cloud-based services are used, or malicious acts affect the system whether through error or through a targeted attack. Procedures need to be in place and appropriate layers of protection implemented to ensure the defined scope is resilient when impacted

from beyond the boundary of its assets [143]. Furthermore, methods for authorising connection to networks and devices or permitting changes to configurations need to be effective and appropriate in a real time operational environment.

## 8.6 Cooperation in managing supply chains

While cybersecurity capability can be built into products, the end-to-end integrated solution needs to be effectively secured involving people, processes and technology. There is an inherent need to integrate skillsets to achieve cybersecurity. Implementing the NIS Directive has necessarily involved bringing together different parts of an organisation to identify the assets in scope and set in place a continuous process for protection, detection, response and recovery. Ideally, this requires a synthesis of IT and OT expertise with sector specific knowledge and in addition the suppliers' deep knowledge of their products and services. The following section explores insights from supply chain management literature on coordinating and influencing supply chains.

### 8.6.1 Building Collaborations

Appropriate collaborative strategies involve both social and technological concerns to meet technical requirements and integrate relevant processes between the organisations involved. Building inter-organizational relationships with suppliers is something to be fostered over time to motivate their participation in collaborative behaviours. Such collaborative effort provides a considerable mediating role in achieving supply chain performance [146]. Several industry interviews shared the opinion that if they had to resort wholly to contractual agreement, it would feel like a failure. Their emphasis, particularly with critical suppliers, was on a mutually supportive relationship and a trusted partnership. This mirrors a study of international procurement where contracts were in place in most cases but were considered less important than clear communication to agree common perceptions and expectations throughout the relationship. Close working relationships were more important than a contract in effective partnership over time. A mutual commitment showed the potential to achieve more than formal agreements [147].

Instead of suppliers acting with self-interest in supply chain systems, Shin and Park demonstrate the importance of a broader awareness of a supply chain system and a mature partnership development to achieve greater confidence in the resiliency of the supply chain.

They identify the following attributes as desirable for all supply chain members and forming key elements of resilience capability and improving a firm's ability to recover from unexpected events:

- Common interest, a collective goal, going beyond self-interest.
- Mutual respect among supply chain partners, competencies and potential for achievement are recognised.
- Deepening trust, meeting operational standards, displaying goodwill towards the partnership.
- Interaction obligations, participation in formal and informal communications among partners for supply chain management activities. A lead firm influencing actions and behaviours of supply chain members to improve capabilities. [148]

Rather than raising maturity level generally, it is important to align improvement in capability with the actual risk exposure to ensure investments are proportionate i.e., through matching the level of risk and vulnerability with appropriate capability to focus investment and effort on actual resilience gaps [149]. This concept of a balanced resilience has also been extended to include the supply chain network [150]. However, there are challenges in knowing the actual risk exposure and the likelihood of incidents and proving whether a cybersecurity investment has been a worthwhile prevention, particularly if there is an absence of incidents. Cooperation is important to bring together information on the latest trend of attacks, along with an understanding of the potential impact, and having preventions in place to minimise these types of impact.

### 8.6.2 Reducing Overhead of supply chain coordination

Attempting to control entire supply chains of cyber secure activity would be a vast and costly undertaking. A more achievable endeavour is to strategically decide what aspects to control and what to let emerge. Choi points out the differences between control and emergence in managing supply chains as complex adaptive systems. The use of control mechanisms involves a formal oversight of suppliers with contractual arrangements and adherence to common standards for more predictable outcomes. Emergence, on the other hand, is where more autonomy is given for local decision making and emergence of the required outcomes is encouraged through positive feedback. Choi proposes that companies managing their supply networks through both control and emergence, outperform those that focus on only

one of these approaches. This entails controlling the overall direction while remaining vigilant in observing what emerges, to make appropriate decisions and changes. Also, encouraging creativity and adaptability in the supply network reduces the coordination cost of a supply network. Choi suggests controlling several tiers deep only for a few critical areas and otherwise allowing the supply network to emerge through empowering top tier suppliers to manage their suppliers [151].

Pass through clauses in contracts with Tier 1 suppliers require the supplier's suppliers to have the same protections in place and the contracted supplier is held responsible for compliance with this clause. These clauses typically only reach Tier1 and Tier 2 suppliers [152]. Coordination of a 'cluster' of suppliers is more realistic than oversight of multiple tiers in the supply chain. Via a lead organisation this is coordinated from a strategic level with a focus on capability and agreed goals, using metrics as an enabler [153]. Roseira's research into supplier networks identifies the ability to recognise the potential in each supplier relationship and diffusing this to other supplier relationships as being of central importance in managing portfolios of suppliers [154]. Addressing actors beyond tier 1 of the supply chain through interactions among multiple actors in a supply network, more commonly leads to resilience to supply chain events [149].

The interconnectedness of supply chain actors requires a holistic approach to resilience. Knowledge created and shared among supply chain partners to build a 'capacity to adapt' to continuous change will allow the whole supply chain to become more resilient. Colicchia recommends "a holistic and extended approach". Awareness training should go beyond the boundaries of the workplace to appreciate the extent of impact because human behaviours can affect the whole supply chain network[150]. Keegan recommends creating opportunities for cooperation among private sector organisations and public-private cooperation through government involvement in industry working groups, creating forums to enable collaboration across organisations and countries [155]. Examples of such collaboration are described in Section 8.8.

## 8.7 Perspectives on Implementing NIS

### 8.7.1 Policy Perspective

Government departments have defined responsibilities and set expectations by providing NIS Guidance and a Cyber Assessment Framework (CAF). By describing indicators of good practice [114], the CAF shows the outcomes to be achieved within each of the principles previously shown in Figure 16.

The evidence supporting the original NIS intervention showed that only 13% of organisations were setting cybersecurity standards for their suppliers to meet; and during 2017 19% had experienced a breach that resulted in a material loss [156]. The potential benefits expected from implementing the NIS Directive, at the outset in April 2018 included the following [157]:

- A reduction in risks to essential services due to the improved security level.
- To improve the cybersecurity of network and information systems (NIS) underpinning essential services.
- To reduce the likelihood and impact of security incidents.
- To also reduce breaches/attacks that are below the Directive thresholds.
- A 5% reduction in number of organisations with a breach or attack was assumed.
- Common security requirements for all market operators.
- The exchange of information and coordination of actions.
- To improve advice and incident response for OES through international cooperation and information sharing.
- Extended benefits were expected to be “substantial where even just one significant incident is prevented” due to potential impact on the wider economy if essential services and network and information systems become unavailable.

There was an emphasis on number of incidents and an expectation that implementing the NIS principles would reduce the number of incidents. However, it was also observed that it is difficult to determine whether implementing security measures will result in a reduced number of breaches. The cybersecurity breaches survey of 2020 shows that breaches and attacks have increased in the last 3 years [158]. Industry feedback during the NIS Review also confirmed the cyber threat level has increased. Fewer negative impacts have been experienced from those breaches so the resilience to attacks appears to have improved,

however continuous improvement is not evidenced, with policies and processes put in place to meet new regulations being maintained rather than enhanced [158].

In 2020 the UK proposed some amendments to their NIS Regulations that showed a move away from penalties. The penalty bands have been revised and a notice of intention to impose a penalty must be given by CA first. This preference was also expressed in interviews through discussion of the 'use of regulatory judgement' while assessing compliance and the intention to 'lead with a carrot more than with a stick'. The supply chain issues have a wider impact than just NIS organisations so Policymakers are looking separately at the role of government in reducing supply chain risks at scale; and what would constitute effective support from government with managing the supply chain risks that OES are currently responsible for [159].

### 8.7.2 Regulator Perspective

This section captures the perspective of CAs, gathered from interviews, along with some examples of specific approaches. A comparison of CA approaches to NIS oversight is provided in Table *21*. An analysis of these approaches is published in the following reference and was presented at the International Conference on Cyber Situational Awareness, Data Analytics and Assessment in 2020:

Tania Wallis, and Chris Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-10, doi: 10.1109/CyberSA49311.2020.9139641

Utilising the CAF from NCSC and based on likely threat scenarios, CAs set expectations on OES with a CAF profile for their sector, using red/amber/green notation to highlight the priorities to be achieved. CAs assess the performance of OES to decide a priority for audits and inspections. A range of parameters are used for this including:

- Likely consequences or impact, of an OES being non-compliant.
- Safety considerations.
- Self-assessment of OES.
- Previous knowledge of the facility.
- Size of facility and importance to the sector.

| | Competent Authority 1 | Competent Authority 2 | Competent Authority 3 |
|---|---|---|---|
| Expectations on OES | CAF profile of NIS outcomes to be achieved. | Assess safety and cybersecurity risks together and take action to mitigate the highest risks. | Achieve a baseline capability defined in sector CAF. |
| Safety and cybersecurity | Separate safety and cyber teams. Gradual integration in longer term. | Integrated approach to safety and security. | Focus on cyber causing safety impacts to operational systems. |
| Planning inspections | Assess risk and complexity of facility & latest performance review. | Screening of self-assessments and improvement plans decides the priority for inspections. | Focus on cross-sector awareness raising and establishing baseline security requirements. |
| Auditors | Outsourcing audits through accreditation of cyber professionals with OT and ICS experience. | Building cybersecurity capability into existing regulatory role. Inspecting compliance level and setting actions to improve compliance. | Cybersecurity being integrated into existing inspectorate role. |
| Overseeing the changes | OES to notify changes in NIS scope or changes of supplier to CA. | Scope definition includes requirements of both safety and cybersecurity regulations. | Offering cybersecurity training to OT staff. |

| | | | |
|---|---|---|---|
| Supply Chain | Compiling list of suppliers and what is being supplied to OES. Responsibility is on OES to secure the supply chain aspect of their essential services. | Supply chains are one aspect of a considerable new implementation effort. OES must assure cybersecurity capability of organisations interacting with their NIS scope. | Awareness raising through supply chain briefings for whole sector. |

Table 21 Comparison of CA approaches to NIS

One CA is using a matrix approach to assess the complexity of different facilities. They assign a complexity level to decide which sites they need to audit. They also decide how much time each facility should be given by auditors based on their latest performance review. On-going improvement and therefore the frequency of audits is also determined through this performance-based oversight.

CAs expect operators to be actively sourcing threat information, to having ongoing vulnerability and threat awareness and a decision-making process to consider new threats at the level of impact. The consequences of new threats are considered alongside measures that are in place to decide necessary improvements and likely effects. The end user is expected to tie it all up, the supply chain vulnerabilities and latest threat intelligence into a potential impact on their deployment environment, to conclude how to respond.

CA consider a range of parameters when assessing sites including the safety impact for the site and the community around. They inspect their NIS sites against all the NIS contributing outcomes from A1a through to D2, relative to the CAF profile they have set for their sector. An example from one CA shows each site is given a score and the extent of their NIS compliance is assigned a category from 1 to 6 as shown in Table 22. The scores help to decide appropriate enforcement levels, for example where compliance has some gaps, a letter specifying actions to be resolved is provided with follow up to ensure actions are implemented. Where compliance is poor, formal legal powers are exercised to enforce the required compliance. 'Regulatory judgment' is also applied to their response, through the CA knowing the site history, realistic expenditure such that an agreed approach can be reached.

| OES Score | OES Category | Consequence from CA |
|---|---|---|
| **10** | Beyond NIS Compliance | |
| **20** | Fully NIS Compliant | |
| **30** | Broadly NIS Compliant | Action to resolve |
| **40** | Poor Compliance | Action to resolve |
| **50** | Very Poor | Formal enforcement |
| **60** | Unacceptable | Formal enforcement |

Table 22 example of NIS Compliance categories being used by CA

The supply chain aspect is in its early stages of maturity. NIS sites broadly know who their suppliers are, and are setting baseline requirements with control system and safety system vendors but these are not in contracts yet so formal assurance of suppliers is work in progress. Big suppliers of control and safety systems have a strong awareness of how cyberthreats can affect their equipment. More recent control systems installations having security included by default. There is less understanding among sites on how to improve security around legacy systems. Actions and enforcements have enabled changes in this area to improve processes and network architecture, with OES engaging with their supply chain as they progress this.

There is a wide range of situations with the sites, some more proactive or with more resources to improve compliance, others tend to wait for CA visit and then make the necessary changes. Some sites are heavily committed to one supplier, using the same vendor for control and safety systems for an integrated solution and consistency with support and spares. Other sites are using a range of equipment requiring systems to be integrated by a different supplier and involving a more disparate and complex cybersecurity solution.

Despite a quantity of outsourcing, the legal duty for cybersecurity sits with the OES. They are expected to be an 'intelligent customer', to know enough to ask the right questions and set the required expectations on suppliers. This can be challenging for smaller sites with fewer resources for this. In some cases, it comes down to one person having responsibility for safety and security, managing changes and making improvements and also being competent in 3rd party assurance.

While most vendors and suppliers have some understanding of cybersecurity issues and that they need to be aware of vulnerabilities in their systems, the regulation has been necessary to push the end users into setting this into contractual arrangements. Some level of standardisation of expectations on the supply chain would be useful, as the range of issues is largely similar for end users and suppliers. A certification process would assist end users to understand the security capability in products and services they are using and demonstrate assurance of vendor solutions through validation by an independent entity. The EU Cybersecurity Act is introducing a scheme to certify devices and services. This will involve third party certification of ICT products at two security assurance levels: 'substantial' and 'high'. It also includes certification of Protection Profiles, being an implementation-independent set of security requirements.

### 8.7.3 Perspectives of Operators of Essential Services (OES)

Operators of Essential Services (OES) are implementing the NIS principles and are required to report incidents that affect the delivery of their essential services. The interviewees expressed that having obligations under the NIS Directive has given OES a strong focus to improve their cybersecurity capability and raise awareness in their organisations and essentially to achieve support at Board Level for making the necessary improvements. Nevertheless OES, in general, have limited resources for overseeing supply chain risks and, as individual organisations, can often lack negotiating power with suppliers [160].

OES are managing cybersecurity across multiple suppliers and updating supplier contracts is a gradual process. Their visibility of supply chain cybersecurity is limited such that incidents in the supply chain may not be notified to an OES. In some cases, there is a low cybersecurity maturity among available suppliers or even dependency on a single supplier for essential product. OES working individually appear to lack real influence to demand greater levels of assurance. In addition, improving the diversity of suppliers may not be more resilient if different suppliers share common components or the same operating system.

During the procurement process, questionnaires are sent to potential suppliers to understand their cybersecurity maturity level. The suppliers' responses are considered, alongside other business risks, during procurement decisions. The questionnaires being used are predominantly assessing a supplier's cybersecurity posture as a company by looking at

how cybersecurity risks are managed; if security policies and processes are implemented; and how effective they see their cybersecurity controls to be.

However, the residual risk that the OES is carrying relates to their cyber risk in operation so the cyber-assurance of the supplier's product or service needs to be the focus, more than the supplier company itself. These questionnaires are informing risk decisions inside the operator on criticality and importance. It is therefore necessary to look at the context of an OES deployment and the impact a supply chain event would have in this specific OES environment, and to know how important that product or service is to the business function and to establish the extent of dependency on that supplier. By also looking at the degree of access a supplier has to sensitive assets, this further paints the picture of how exposed an OES is to a supplier's cyber risks.

| **Key challenges faced by OES in securing Supply Chains** |
|---|
| OES have a limited ability to negotiate security requirements from suppliers. |
| OES lack choice in selecting suppliers – they shoulder the risk of low cybersecurity maturity among available suppliers. |
| Difficulty obtaining supplier commitment to improvements following risk assessments. |
| Facing challenges with inserting cybersecurity requirements into established contracts at renewal. |
| Limited resources to integrate cyber security requirements and expectations into all outsourced activities. |
| Visibility of sub-contractors is very limited. |
| Supply chain incidents may not be notified to the OES. |
| Uncertainties around security status of products – there is lack of transparency on through life support. |
| Uncertainties over shared responsibilities in operations, complex dependencies. |

Table 23 Supply Chain challenges of OES

Table 23 highlights the key challenges discovered that OES face in securing their supply chains to comply with NIS. Due to the limited influence an OES has working at this on their own, there has been a growing interest to collaborate. For example, to discuss shared security requirements that could be built into suppliers' offerings rather than cybersecurity

add-ons being sold separately to each OES; to have cybersecurity included in technical requirements so that the fundamentals are in place and it is priced with cybersecurity included. OES are looking for support beyond initial warranty, for the life of an asset. There is a lack of clarity and transparency on the through life support for the security of products leaving uncertainties around the security status of products. While the Operators of Essential Services are the necessary focal point of NIS, it is a complex task for OES to assign appropriate requirements and responsibilities onto suppliers and systems integrators. Suppliers are also receiving multiple different questionnaires from different operators to assess their cybersecurity capability which is reducing the efficiency of supply chain assurance activity for all parties.

While NIS has brought a one company approach to improving cybersecurity one OES at a time. There are areas where a combined approach needs to be facilitated. It would involve a significant overhead of cost and time for each OES to attend to the cybersecurity of their entire supply chain, or even just the critical suppliers on which their essential service depends. The NIS implementation has mobilised some collaborations to work towards NIS outcomes more effectively, highlighting the importance of partnership to achieve cybersecurity. Recent working groups have been fostering collaborations to this effect. These are described in Section 8.8.

### 8.7.4 Supplier Perspective

The weighting of this perspective is towards suppliers with a strong presence in CNI and who are focussed on cybersecurity hence they were more willing to participate in interviews. Table 24 outlines some of the key challenges raised by suppliers.

Suppliers that offer a good standard of cybersecurity in their offering can be penalised when cybersecurity is considered, but not prioritised, in the procurement process and where there is an emphasis on keeping costs down. Also, where cybersecurity requirements are not adequately defined by OES, suppliers are left to estimate the risk appetite and cybersecurity level they need to meet for their customer's context.

| Key challenges faced by Suppliers |
| --- |
| Suppliers are receiving multiple different questionnaires from different operators to assess their cybersecurity capability. |
| Cybersecurity is considered by OES but not prioritised in their procurement process. |
| An emphasis on keeping costs down is encouraging an installation that is right for today rather than future proof infrastructure. |
| Where cybersecurity requirements are not adequately defined by OES, suppliers are left to estimate the risk appetite and cybersecurity level they need to meet for their customer's context. |

Table 24 Challenges experienced by Suppliers

Suppliers need OES to agree and provide common requirements per sector to ensure basic security is in place across all supplier offerings. OES jointly agreeing and providing common security requirements in one sector has been very well received by suppliers. For that sector, it created a more level playing field and a standard expectation that prevented a race to the bottom on security for best cost solution. Suppliers are showing a preference for their market being driven by the cybersecurity requirements per sector, defined by OES. However, even at the requirements stage, OES can require dialogue with their suppliers in order to fully define their requirements, to bring a supplier's deep knowledge of their product together with operator's understanding of the environment it is deployed into. There are concerns among OES that their security requirements could force a significant technology change. Large suppliers know their equipment is embedded into an OES so they can charge for security improvements because it would be a massive undertaking for the OES to change supplier.

Suppliers are seeing an increasing interest in having cybersecurity capability within their products coming from the manufacturing sector. However, in NIS regulated sectors, they see a cultural aspect that is slowing down cybersecurity improvements. In particular, there is an intense focus on costs in one sector that encourages an installation that is right for today, rather than deploying future proof infrastructure. Where cybersecurity responsibility has been given to IT, there can be a limited understanding of the extent of their cybersecurity responsibilities within the operational environment.

While the responsibility for implementing and complying with the NIS Directive is with the OES, there is reluctance from suppliers to take on cybersecurity responsibilities that sit in the context of OES deployments. However, there needs to be a fair set of expectations on suppliers for example to have cybersecurity designed into their products and services and the OES take responsibility for how cybersecurity capability is configured and used in their environment. Some collaboration and negotiation will be required to agree what can be expected and included as standard within a supplier offering and what is considered as additional and chargeable as an extra. Both the operators and suppliers need more clarity on the cybersecurity practices to adopt and a shared understanding of the current and emerging cybersecurity risks, as increasing digitalisation progresses.

## 8.8 Examples of Interorganizational Cooperation for Cybersecurity

Two-way relationships between operators of critical infrastructure and the suppliers of products and services they use are an important consideration. Cyber security issues in the supply chain can introduce risks and potential operational impact that the operator needs to manage. An operational incident could also impact the reputation of a supplier. The translation of an operator's regulatory obligation into security requirements of suppliers can to some extent be incorporated into commercial contracts and in this way allocate some responsibilities to suppliers. A continuing relationship with suppliers is necessary to support cybersecurity needs such as patching of software and incident response arrangements and particularly throughout the lifecycle of products. Consideration of how the relationship will endure over time, the potential needs in the longer term and how they can be met through likely changes [143].

### 8.8.1 Unified supply chain assurance

Although the focus of this paper has been on the UK response to NIS implementation, the concerns extend across national borders. For example, the European Air Traffic Management (ATM) industry has worked together to produce a unified approach to supply chain assurance. Table 25 shows the supply chain aspect of the maturity model that was developed to compare the suppliers to Air Navigation Service Providers (ANSP). The levels define a progression from partial to full oversight of suppliers, and from self-assessment to carrying out compliance checks. The eventual aim is to achieve an adaptive security that supports regular updates to requirements and independent assessments of suppliers.

| Supply Chain Risk Management | |
|---|---|
| The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has in place the processes to identify, assess and manage supply chain risks. Appropriate levels of trust are established with data exchange partners. | |
| **Level 0 non-existent** | No complete overview of all suppliers / partners. |
| **Level 1 partial** | Some requirements placed on some suppliers and agreements with some partners; partial and informal understanding of supplier/partner cyber-maturity. |
| **Level 2 defined** | Minimum set of requirements placed on all critical suppliers and agreements with partners, with mostly self-assessment for compliance. |
| **Level 3 assured** | Requirements placed on suppliers with proportionate compliance checks and processes / penalties /measures for non-compliance. |
| **Level 4 adaptive** | Independent reviews / audits / assessments supporting regular updates of requirements against new good practices. |

Table 25 Supply Chain category of ATM Maturity Model [161]

Figure 18 provided an example for presenting the comparison of suppliers in order of maturity. The intention was for ATM operators to progress towards achieving full oversight of their supply chain by following this unified approach. Since the introduction of this unified maturity model and the NIS obligations, there has been some progress with the oversight of supply chains through achieving a partial understanding of supplier maturity. However, to take actions towards improvement required a gathering of the key issues from operators so that visits and workshops with key suppliers could be arranged at a country level coordinated by the CAA.

| Function | Category | ANSP | Supplier 1 | Supplier 2 | Supplier 3 | Supplier 4 | Supplier 5 |
|---|---|---|---|---|---|---|---|
| LEAD AND GOVERN | Leadership and governance | 3 | 3 | 3 | 2 | 1 | 1 |
| | Cyber Security Management System (CyberSecMS) | 2 | 3 | 2 | 2 | 2 | 1 |
| IDENTIFY | Asset Management | 4 | 4 | 3 | 2 | 2 | 1 |
| | Risk Assessment | 1 | 3 | 3 | 1 | 2 | 1 |
| | Information sharing | 2 | 3 | 2 | 1 | 1 | 0 |
| | Supply Chain Risk Management | 2 | 3 | 3 | 2 | 1 | 0 |
| PROTECT | Identity Management and Access Control | 3 | 4 | 2 | 2 | 3 | 2 |
| | Human-centred security | 1 | 3 | 3 | 2 | 2 | 0 |
| | Protective Technology | 3 | 4 | 2 | 3 | 1 | 1 |
| DETECT | Anomalies and Events | 3 | 2 | 2 | 2 | 2 | 0 |
| RESPOND | Response Planning | 2 | 3 | 3 | 3 | 0 | 0 |
| | Mitigation | 3 | 3 | 2 | 2 | 0 | 1 |
| RECOVER | Recovery Planning | 3 | 3 | 3 | 1 | 2 | 1 |

*Figure 18 Unified approach to supply chain assurance for ANSI* [161]

### 8.8.2 Collaborative Supplier Assurance

The effective implementation of the NIS Directive and resulting improvement in cybersecurity across critical infrastructure is contextually dependent on the knowledge of each operator's own environment and unique deployment of infrastructure. The necessity of focusing the NIS Directive on the activities of individual organisations, has produced an array of individual responses. This was an important aspect of the NIS Guidance, by providing outcomes to aim for rather than a checklist of actions to ensure the efforts were towards the reduction of risks for each operational facility. As this effort rippled out, a knock-on effect to suppliers was receiving multiple different questionnaires from their customers to assess their cybersecurity.

This overhead of activity, for both OES and suppliers, to understand the risks in the supply chain can be reduced through improved cooperation. Groups of OES in the energy sector were discussing their common security requirements with suppliers, one at a time. This developed into a supplier assurance working group to agree a common approach for the whole energy sector, supported by Government. This collaboration has produced and agreed a set of guidance for the sector on supplier assurance. This working group is also working on a code of practice and partnership approach with suppliers to the energy sector.

Sector collaborations can improve OES leverage with larger suppliers. Agreement of common security requirements per sector by OES can provide a more level playing field for the supplier market. Defining clear security requirements at a whole sector level should improve negotiations with sole suppliers to meet them, despite not having the competition within the market to improve their security provision. Where possible a more centralised coordination of supplier assurance is recommended by introducing a shared assessment process within each sector with one assessment per supplier to improve efficiencies in this area. A trusted intermediary in such partnerships has been particularly effective to establish a picture for the sector, by anonymising information from individual OES.

### 8.8.3 Centralised supplier assurance

The Scottish Government have provided an example of a centralised supplier assessment process within the health sector through their digital telecare security assessments [162]. The key aims and outcomes have been as follows:

- for consistency and to reduce the burden of providing evidence to multiple parties.
- to increase supplier engagement.
- to reduce the cost of supplier assurance.
- to use a risk-based assessment of product/service and supplier company.
- to build trust between the assessor and suppliers.
- to establish a non-disclosure agreement due to vulnerabilities identified during the assurance process.
- to offer guidance, as necessary, for suppliers to achieve the required standard.
- to agree timely improvements where required.

### 8.8.4 Managing software vulnerabilities

Complex supply chains can propagate vulnerabilities. Without a software bill of materials (SBOM), it is more difficult to know if vulnerable software is in a device. Risk mitigation requires a detailed and dynamic asset inventory to hold information for each device, on vendors, operating system, firmware version etc. The risk surface also depends on the context surrounding a device so the actual impact of a vulnerability depends on the environment a targeted device is implemented in [163].

New software vulnerabilities can be embedded within many components and users need to know if they will be affected by a software vulnerability through regular assurance of a SBOM. SAFEcode produced an assurance model that includes:

- security – anticipate and address vulnerabilities during design.
- integrity – in sourcing and creating software components, address the likelihood of vulnerabilities in delivery of software.
- authenticity – provide ways to assure and differentiate genuine products from counterfeit products. [164]

Edison Electric Institute (EEI) with U.S. Department of Commerce's National Technology and Information Administration (NTIA) is at the nexus of a discussion with software vendors, security experts and asset owners. NTIA are facilitating this effort with different sectors: health, energy, automotive and banking with an emphasis on cooperation rather than using regulations. This involves the application of SBOM as a tool to minimise supply chain risks, to know the components of software so that vulnerabilities become known and to work with suppliers to mitigate them. Sector specific engagement will uncover the importance of an element to that sector and potential impact to a sector of a vulnerable supply chain component. Cross sector engagement will also be necessary because different CNI sectors are likely to have the same software components embedded in their systems. The intention is to develop a shared vision and language working with individual sectors first and to work towards creating machine readable methods for fast automatic assessment of impact and to enable sharing across sectors [165].

### 8.8.5 Cyber exercises with suppliers

A recent victim of attacks reported that exposure to incidents has significantly increased awareness across the organisation. Any phishing attempt “echoes” through our organisation, sharing of near misses or potential incidents happens much faster. Exercises in responding to cybersecurity events can provide a holistic experience to identify capability gaps from people, process and technology perspectives. Whole sector cyber exercises have increased awareness of the need to respond collectively to cyber events and the benefits of collaborative working across OES, suppliers and government. Participants in the cyber exercises appreciated gaining visibility of the bigger picture and understanding of how local decisions can impact the wider sector. It exposed the need for a coordination role, by

Government or an industry body, to deal with sector wide incidents, rather than being treated as several incidents by many separate organisations. It raised supplier awareness of the necessity to support CNI with NIS compliance and even to revisit contractual agreements with individual OES to consider extending them in some areas towards whole sector agreements.

## 8.9 Enhancing cooperation in securing supply chains

In addition to specific NIS Guidance, the UK NCSC provide general supply chain security guidance to improve overall resilience and reduce business disruptions [166]. This is offered in four stages as listed in Table 26. This research recommends some enhancements to this guidance, based on the experiences of implementing NIS across critical infrastructure, that are listed in Table 26 and elaborated below. These recommendations aim to improve effective interworking across supply chains.

| **NCSC Supply Chain principles** | **Enhancements to Supply Chain Guidance** |
|---|---|
| Understand the Risks | Emphasis on risk reduction |
| Establish Control | Driving improvements |
| Check your arrangements | Measures & Performance |
| Continuous improvement | Mutual Commitment & Accountability |

Table 26 Enhancements to Supply Chain Guidance

### 8.9.1 Emphasis on risk reduction

Rather than an emphasis on increasing maturity or adding capability, it is important that decisions continue to be based on reducing risks and minimising the impact of incidents. To really know and understand the supply chain risks to critical infrastructure requires improved information sharing and cooperation across industry and across supply networks. This would assist with understanding the latest threat picture, of incidents and near misses, and with identifying the impact of vulnerabilities at a sector level, such as software vulnerabilities in supply chain components.

In addition to the emphasis on managing and reducing risks for the assets relevant to delivering essential services. Further attention could be given to the impact beyond NIS identified assets, by considering the cyber resilience of the entire organisation, as a whole,

to include the human and process effects on these critical assets and the delivery of essential services.

### 8.9.2 Driving improvements

While the NCSC supply chain guidance places attention on establishing control of the supply chain, this research has highlighted some challenges for OES working alone with achieving that level of control. Therefore, balancing controls with cooperation is recommended, see Figure 19, and approaches to achieving this have been explored. It is essential to establish the new behaviours that will drive improvements and reduce the risks. Sector collaborations can improve OES leverage with suppliers. For example, by OES together agreeing common security requirements, to lead their sector's supplier market. A combined supplier assurance process can also reduce the overhead of this activity on both OES and suppliers. More resources will be required to consider essential components of the supply chain and to facilitate an assured software bill of materials SBOM and know the impact of vulnerabilities in supply chain elements.

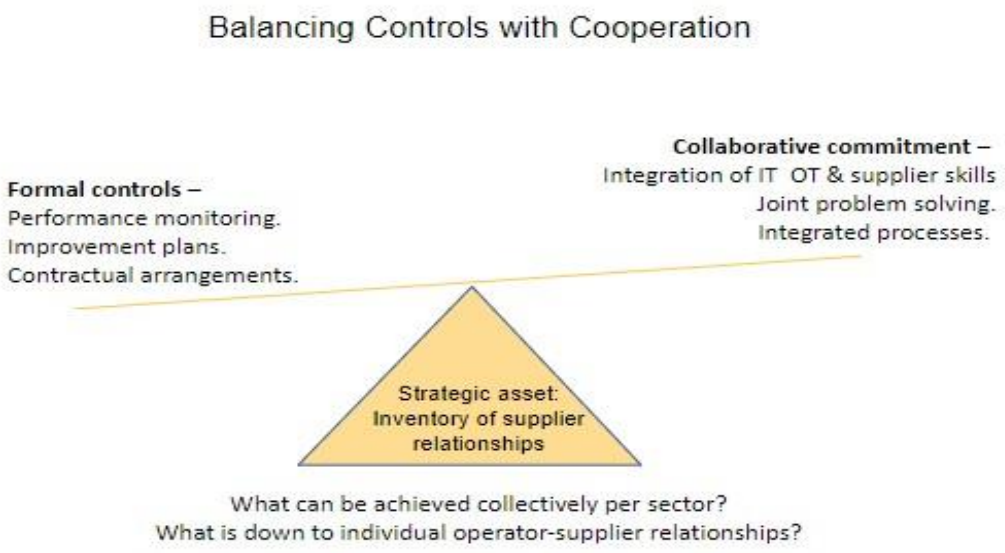


*Figure 19 Balance between control and cooperation*

In addition to holding an asset inventory that covers hardware, software, and connectivity to support security initiatives such as patching and assessing impact of vulnerabilities. An inventory of supplier relationships is recommended to cover the human and process elements as well and recognise the supply chain as a strategic asset to be managed. Again,

sector wide cooperation could establish the foundation for ongoing relations with suppliers through agreeing a sector code of practice. The individual operator-supplier relationships can then focus on more contextual needs related to OES deployments in their unique operational environments.

Understanding the areas of commonality indicates what can be achieved collectively per sector. This will require Government support for the necessary collaborations, for example cyber exercises involving suppliers to improve integration of incident response processes. Governments can positively impact the long-term goal of cybersecurity improvements by supporting or facilitating such interorganizational cooperation.

### 8.9.3 Measures & Performance

A collective responsibility and mutual commitment to cybersecurity is the means to establish the required behaviours and improvements. By understanding the potential impact of supply chain components on CNI, suppliers can be categorized as critical, important, medium or low priority [160]. In order to track and measure improvements, points of governance or points of influence need to be identified within the supply network, where controls or cooperation are required with critical and important suppliers.

Similar to the 6-monthly review of NIS improvement plans with OES that are overseen by the CA, there also needs to be a regular review of commitments to maintain accountability with suppliers. To be more efficient on time and resources, and with the required interorganizational cooperation in place, this can largely be an attention to sector wide commitments from the supply chain. Then individual OES attention can be on their more contextual and tailored requirements. Agreeing shared language will also be necessary to facilitate the collaboration across organisations.

Table 27 shows examples of actions that all depend on effective cooperation. Using a balance of lagging and leading measures to assess performance and guide improvements, will inform future decisions while learning from events.

| Lagging indicators<br>to learn from the past: | Leading indicators<br>to inform decisions: |
|---|---|
| • Reporting of incidents and their impact.<br>• Ability to recover from events.<br>• Sharing of lessons learned to plan improvements.<br>• Responsible disclosure of newly discovered vulnerabilities.<br>• Tracking the resolution of vulnerabilities or the required mitigations. | • Knowing what to improve, improvement plans assessing performance. The subjective assessments assigning red, amber or green could instead be linked to more specific and measurable milestones in the improvement plans.<br>• Consider what-if scenarios and potential disruptions, emerging threats, early signs of vulnerabilities, and near misses. This needs improved coordination and cooperation to guide these preparations.<br>• Improved visibility of dependencies on supply chain components, to prevent supply chain effects cascading.<br>• Understand the residual risks being carried by OES to prioritise their mitigation. |

Table 27 Cooperation in performance

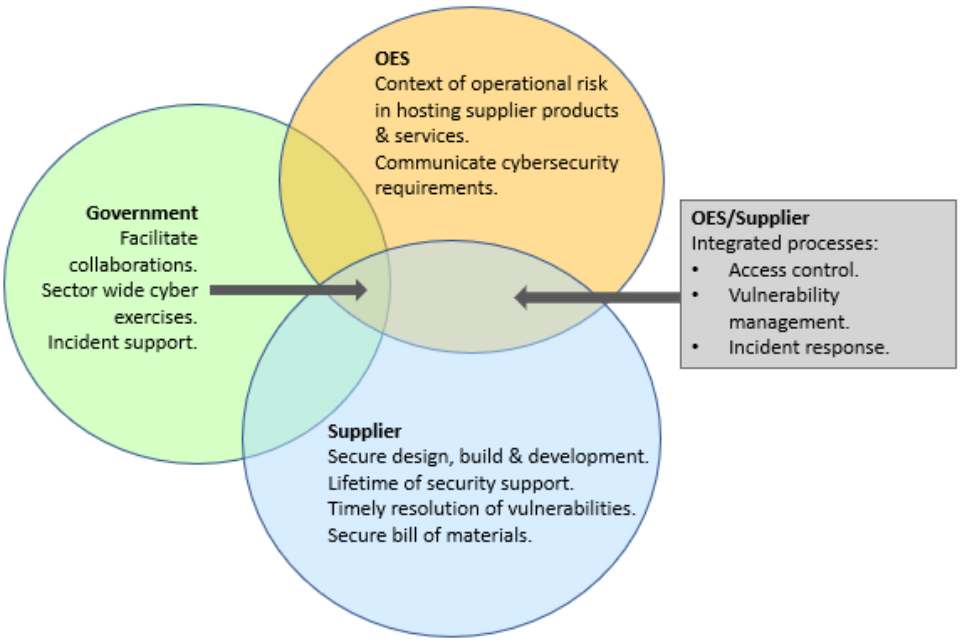


*Figure 20 Mutual Commitment required from Public & Private actors*

## 8.10 Mutual Commitment & Accountability

Figure 20 demonstrates the collective commitment that is required across public-private partnerships involving OESs, Suppliers and Government departments.

A code of practice per sector would establish the commitment to action. A definition of and regular review of commitments will maintain accountability among sector participants. For example, broadening the current individual OES improvement plans by also overseeing sector improvements and mutual commitments in the interorganizational space. In the longer term, it is a continual adaptation to the evolving situation, by the whole supply chain network, that will improve resilience to cyber events.

## 8.11 Balancing control with cooperation mechanisms

This research has evaluated public and private sector experiences with implementing the NIS Directive, and provided examples of effective cybersecurity collaborations. It has presented some enhancements to supply chain guidance to assist with reducing cybersecurity risks to critical infrastructure and emphasizes the need for greater interorganizational cooperation.

In particular, the OES context of deployment & operational impact makes it harder for OES to share cybersecurity responsibility with suppliers for products and services that OES are hosting in their own operational environment. The ability of OES to make formal upfront arrangements with suppliers through contractual agreements is limited, not least due to the adaptability to an evolving situation that is required. Fostering trusted partnerships and mutual commitments is equally important and even has the potential to achieve more than formal agreements.

The regulatory controls introduced by NIS need to be balanced with a more cooperative approach through Government support for the necessary collaborations that will drive improvements. It is also important that common language, standards and frameworks are used to promote shared understanding along the supply chain. To incentivise suppliers, a greater clarity on sector cybersecurity requirements is needed to set the level and lead supplier markets.

This research recommends a combination of control and cooperation mechanisms, developed from researching industry experiences and supported by supply chain

management literature. To build and maintain the required cybersecurity capability to secure essential services and refine those capabilities in the light of new threats and vulnerabilities; organisations, products, and services must understand their role in critical infrastructure and their place and responsibility in the supply chain.

# 9 Conclusion

This chapter concludes the thesis by outlining the contributions.

Cybersecurity is a shared problem, and it requires shared understanding and partnership to address it. Policy interventions can only focus on the cybersecurity obligations of individual organizations. End to end security, for the technical solutions and services that encompass multiple actors, requires interorganisational responses. The effective transfer of risk between organisations and the dividing up of responsibility and accountability is a challenge. The risks are shared in a technically interdependent solution.

This work has built and exercised interorganisational responses in a number of settings. Practice spaces, formed and led by the author, have enabled shared understandings, trans-professional and trans-disciplinary experiences, and a reorientation of energy sector participants towards more effective cooperation in cybersecurity.

Maintaining this orienting function is necessary, to adapt and reposition, through regular evaluations of continuously evolving environments, and can be facilitated by an ongoing commitment to interorganisational action.

The key contributions of this thesis are as follows:

- Defined and communicated a foundational understanding of the operational context for cybersecurity in the energy sector, from an integrated knowledge space across industry and academia, including IT, OT & Communications.
- Action-based research has built and analysed partnership and multi-actor approaches for a distributed power system with cybersecurity and operational responsibilities across organisational and country boundaries.
- Developed frameworks to support interorganisational responses and supply chain contributions to cybersecurity.
- Orientation of the energy sector towards a mutual cooperation and commitment to cybersecurity, by integration of skills and experience and co-production of useable information and guidance.
- Enhanced multi-actor partnerships with recommendations for further cooperation that aligned with sector and regulatory developments.

The following sections outline the contributions of this thesis in more detail.

## 9.1 An integrated knowledge space to define the OT context of energy cybersecurity

An integrated knowledge space across industry & academia including IT, OT, telecoms, defined and raised awareness of the context of energy cybersecurity by:

- Fostering an understanding of the energy OT context for more applicable solutions, enabling participants from different skillsets to orient and adapt to energy sector transformations.
- Identifying key concerns for Distribution Network Operators on achieving cybersecurity of future energy scenarios.
- Considering the wider engineering solution beyond security.
- Defining the future energy system context for the ongoing design of cybersecurity improvements.
- Evaluating energy sector needs enabled prioritisation of security innovations in the PNDC research programme which led to future work in asset discovery, identification and analysis of asset vulnerabilities, and pen testing of electric power assets.

## 9.2 Developing beyond ISAC information sharing

This research provides an example of the progress, challenges and effort that have built a trusted network and deepened cooperation in cybersecurity among energy sector participants both within Europe and globally. The contributions of this work, listed below, provide a platform for interorganisational response that supports re-orienting to a more secure digitalisation of energy.

- Creating a new context, beyond organisational and national borders, for mutual cooperation, this work provides an exemplar of cybersecurity co-operation between interdependent organisations in the energy sector, within Europe and with international partners.

- Forming practice spaces to co-produce cybersecurity guidance with an energy sector community, to develop the ISAC beyond information sharing, and enable a more integrated cyber capability across different energy sector actors.
- The practice groups synthesising academic and professional skills for Risk Management and Incident Response, to integrate knowledge and experience and co-produce more useable information, resulted in white papers being shared more widely as guidance for the energy sector OT community.
- Proposing a novel solution to build multi-actor situation awareness and integrate a 'trusted hub' of ISAC activities into the currently evolving operational and regulatory situation.
- Providing a combined voice for the energy sector on cybersecurity: an anonymous survey of energy operators was presented to national authorities to commence public-private cooperation for the NIS Directive and consolidate EE-ISAC's presence as a reference point in European critical infrastructure protection.
- Developing the EE-ISAC towards regular information sharing provided a knowledge base to inform guidance produced by ENISA that is assisting the formation of newer ISACs.

Analysis of the ISAC recommended new focus areas. This contribution provides direction for the ISAC to mature from a trusted information sharing network into a more defined and managed role that also demonstrates the importance of translation of cybersecurity to sectoral contexts. It offers an opportunity to integrate their actions into the changing regulatory landscape and cross-border requirements of the continental synchronous grid area:

- To integrate with an evolving operational and regulatory setting by assisting implementation of NIS2 and NCCS.
- Provide sector specific actionable information to utilities.
- Develop further threat and incident analysis capability.
- Attend to interdependencies & supply chain assurance.

- Assess ISAC performance & contribution to sector improvements.

This analysis emphasises the importance of a multi-actor partnership approach to cybersecurity, whether carried out by an ISAC or other entity, that requires a combined governance and facilitation capability, that requires recognition with committed resources from government, academia or industry associations.

## 9.3 Defining collective responsibility in supply chain cybersecurity

A study of interorganisational cooperation within the context of securing supply chains to critical infrastructure includes a cross-industry comparison of the UK's implementation of the NIS Directive, that placed the responsibility for supply chain cybersecurity onto Operators of Essential Services (OES). This research contributes a cross-sector comparison of experiences in Energy, Water & Aviation evaluating the response of different actors to NIS interventions and their challenges in meeting their assigned responsibilities, in particular their ability to oversee supply chain cybersecurity. It proposes further support for partnerships and cooperation across organisations to increase the effectiveness of NIS implementation. Based on results from semi-structured interviews and observations of industry working groups, an approach to supply chain oversight to achieve a balance between control and cooperation is recommended, to improve cybersecurity within industry sectors and across critical national infrastructures. Contributions include:

- A synthesis of perspectives from competent authorities, operators, suppliers and with supply chain management literature.
- Emphasising supplier relationships as a strategic asset due to the mutual commitment to cybersecurity required from all parties - recommending a balance between control and cooperation, such as utilising the formal controls of contractual arrangements, alongside collaborative commitments to integrate skills and processes.
- From experiences of implementing the NIS Directive in the UK, alongside reviews of supply chain management literature, an enhancement to NCSC supply chain guidance is provided, to orient practitioners towards more efficient and effective oversight of supply chain cybersecurity:
    - Emphasis on reducing the impact of incidents.

- Common security requirements & supplier assurance per sector.
- Utilising points of governance in the supply chain, where controls or cooperation are required.
- Regular review of commitments to maintain accountability between operators and suppliers.

The author is currently actioning these contributions through an impact acceleration project that includes co-leading a supply chain cybersecurity community to progress actions on behalf of UK NCSC, involving energy, rail, water, health and aviation sectors.

## 9.4 Orientation & Interorganisational response

A key motivation for this work was the need to establish an orient function, identified in Section 2.2, as a foundation for energy operators to orient themselves among the interdependencies of critical infrastructure, to better understand their place and responsibility to secure assets and services, for their own business and for the energy system as a whole.

Due to participants coming from different points of reference, the governance and oversight of cybersecurity has been evolving as if country and organisational boundaries also exist within the technical solution, which predominantly they do not. As implied in Section 7.5.1 the NIS2 information sharing mechanisms use national borders as a framework whereas the actual operational and technical boundaries differ. The technical boundaries correspond to the European synchronous AC grid area, or the UK National Grid, that is electrically tied at the same frequency, where power supply and demand is balanced in real time. The boundaries of energy companies can be within a nation or operating across borders in the case of larger organisations, all with international supply chains providing components, systems and services into the mix. Hence, this thesis aims to re-orient the energy sector towards a mutual cooperation and commitment to agreed practices, by setting a foundational understanding of the operational context, enhancing multi-actor partnerships and through addressing the multiple perspectives of secure supply chain contributions. This research has emphasised cooperation between interdependent organisations as an essential aspect of cybersecurity governance.

To address the complex interdependencies of CNI Figure 21 proposes an Orientation framework to guide cooperative and reciprocal adjustments by all relevant parties. It recognises there are multiple influences towards reaching the requirements, of the EU NIS Directive and UK NIS Regulations, and defines the high-level engagement activity required to compile a more complete picture and effectively monitor progress. By taking a cross-section of individual and collective contributions, it shows four different views to cover the diverse influences affecting the cybersecurity level achieved. This is described further in the following publication, and was presented at the International Conference on Cyber Situational Awareness, Data Analytics and Assessment in 2020:

Tania Wallis, and Chris Johnson, "Implementing the NIS Directive, driving cybersecurity improvements for Essential Services," 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020, pp. 1-10, doi: 10.1109/CyberSA49311.2020.9139641.

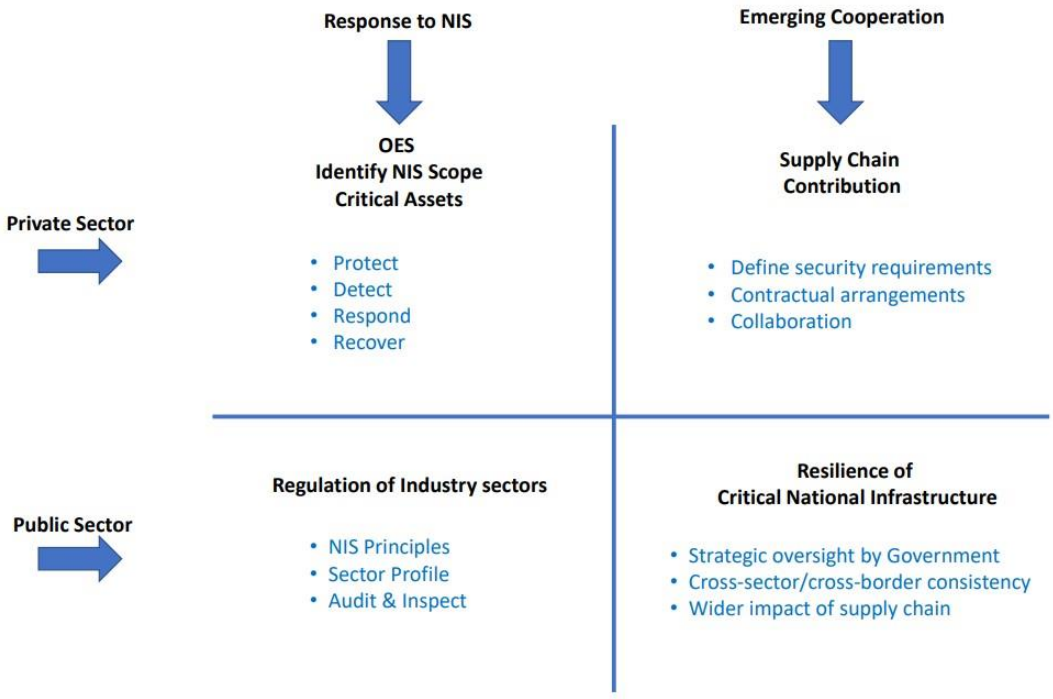


*Figure 21 Emerging Cooperation Framework*

Managing cybersecurity risks essentially requires the ability to identify a change in security risks and to make an informed response to that change. There are multiple levels to this activity. Achievement of the CAF requires an approach to supply chain risk management that prepares essential functions for “subversion by capable and well-resourced attackers” [62].

This level of cybersecurity is currently unachievable by OES working independently and assessed as individual organisations. Fostering assurance collaborations with a consistent approach to managing risks across organisations and supply chains would aid this effort. The regulatory activity underpinning the cybersecurity of our essential services is dynamic, with multiple actors participating. It requires coordination across a distributed accountability and effective communication across actors, to improve their capacity to re-orient to the latest situation, by making more informed decisions while protecting our infrastructure and responding to events.

Cybersecurity is a shared problem which needs shared understanding and partnership to address it. The author's work with OT participants has confirmed there are benefits to adopting common cybersecurity assurance standards and approaches in order to reduce unnecessary duplicated work in operators and suppliers. A collaborative approach establishes a necessary Orientation function and achieves a much clearer understanding of cybersecurity risk by all participants and also helps to overcome information asymmetries in supply chains. The common vision and mission of cyber professionals spurs them to donate effort to endeavours such as the practice groups described in this thesis but will usually require support from their sponsoring organization to resource the necessary activity. To be successful, collaborative groups working on common standards and approaches need a shared mission and must gain individual value from the work. These groups must have committed resources and be able to develop personal relationships to establish trust. A combined governance and facilitation capability, which is typically provided by support from government, academia, institutes, or associations, is essential for such groups to progress significant outputs together.

## 9.5 Outreach

The following summarises some outreach activities that accompanied this research:

- Invited by NCSC to present supply chain research to the UK Cabinet Office & Lead Government departments.
- Regular engagement with policymakers at UK DCMS on supply chains and OT specifics.
- Operator experiences with implementing the NIS Directive were presented to the NIS Cooperation Group's Energy Workstream and EE-ISAC.

- Invited to a Cyber Salon panel by Forum Europe to discuss the NIS Directive and consistency in approach across the European Union, ahead of EU policymakers announcing proposed changes to the NIS Directive.
- EE-ISAC practices were provided to ENISA to inform a toolkit for new ISACs.
- Information sharing requirements were provided to Empowering EU ISAC project for new tool development.
- Presentation to European Leadership Network – to meet their interest in cyber defence of energy infrastructure and security for 'wider Europe' to improve cooperation.
- Co-leading a supply chain cybersecurity expert community, on behalf of UK NCSC, to co-produce further guidance relevant to OT.

## 9.6 Future Work

The organisational context research covered in Section 5 set the foundation for future cybersecurity projects at PNDC including improving incident response capabilities, asset discovery on power communications networks, identification and analyses of vulnerabilities in network assets and penetration testing of electric power assets.

The assessment of EE-ISAC progress and proposal for strategic development of the ISAC in Section 7 can assist other ISACs to also define their role to dovetail with the expectations and needs evolving in their sector. This work has prompted the EE-ISAC Board to begin working towards formalising the future role of the ISAC within evolving procedures and regulations.

The cross-sector research into supply chain oversight in Section 8 has since informed guidance being produced by NCSC. The author has also commenced future work to implement a Supply Chain community that brings together cybersecurity professionals with a shared interest in improving supply chain cybersecurity for Operational Technology (OT) environments. This is fostering the cross-fertilising of cybersecurity experiences between several critical infrastructures sectors including energy, rail, water, health and aviation. Analysis of the uptake and practical use of existing supply chain guidance identified gaps where OT specific guidance is now being co-produced by the group. Understanding and communicating the context of securing cyber-physical systems is another essential

perspective for this community. Examining touch points with the supply chain and identifying potential gaps in communication of cybersecurity requirements and tailoring of implementations towards operational technology contexts. The community aims to provide a partnership framework and to translate experiences into useful guidance to improve cybersecurity levels across multiple contributors to critical infrastructure systems. Table *28* gives an outline of topic areas that are underway for this impact acceleration in Supply Chain Cybersecurity.

With more outsourcing and less visibility into parts of critical infrastructure, there is increasingly less control by single organisations. By implementing a community of interest in supply chain cybersecurity, a pooling of knowledge across the sector is enabling a broader set of participants to have access to appropriate cybersecurity guidance and best practices that are specific to the operational technology and cyber-physical context of energy services. In the context of securing critical infrastructure and services, there's a mix of different aims and risk appetites resulting in a balance to be determined between internal responsibility to address business risks and ensure a business remains viable and the bigger picture of addressing CNI risks. This calls for a framework of engagement addressing individual and collective responsibility. The hosting of the group and the partnering of customer and supplier perspectives is stimulating new capability in supply chain cybersecurity to evolve. It offers a framework to enable the co-production of cybersecurity guidance and practices. It is finding common ground among diverse stakeholders and providing case studies of industry context as interpretations on how to meet the cybersecurity principles provided in NCSC guidance.

| **Topic Area** | Aim |
|---|---|
| **Review of touchpoints with the Supply Chain** | What is the status of the various touchpoints and engagements with the supply chain? Assess the effectiveness of governance/influence of supply chains, through procurement, contractual arrangements and through the lifetime of the product/service. |

| | |
|---|---|
| **Standards** | Communicate what standards are being used to define ICS/OT security expectations, per sector and globally. |
| **Contract and Agreement terms** | Putting ICS/OT relevant security expectations into contractual clauses. |
| **Communicate Current State during tendering** | How to communicate the current state of a system and the security requirements for its target state. |
| **Generic Code of Practice & Partnership (CoPP)** | A framework and rules of engagement to inform CoPP development in individual industry sectors.<br><br>How to establish successful commercial and personal dynamics to make a CoPP effective and valuable. |
| **Supply Chain Cyber Assurance Tools** | A roadmap to help navigate supplier assurance tools and services, categorise their purpose. |
| **Commissioning stage of a contract** | Guidance for managing security during commissioning, potentially a weak phase of the system lifecycle. |
| **Assurance Providers** | What is available in terms of Assurance Service Providers/Shared Assurance - how well do they address OT? |
| **'Procurement Lite' for small companies** | Large and expert teams are not a feasible approach for smaller companies. Produce or recommend 'Lite' versions of assurance standards and processes that can be used by smaller companies. |
| **Incident Response and Management within the Supply Chain** | Where the supplier is a key partner in effective response and recovery, establish clear roles and responsibilities, examine processes, case studies and the use of cyber exercises. |

| | |
|---|---|
| **Joint Security Committee/Supplier Council** | How to create a 1:1 security committee to help govern a particular contract. How to run a security council that includes a company and its supply chain. |
| **Safety & Security** | Investigate Incompatibilities between safety and security. |
| **Reasonable Foreseeable Scenarios** | Use of counterfactuals/what-if scenarios in customer-supplier relationships. |
| **Evolution of NIS** | Support members in understanding the evolution of NIS in UK and EU. |

Table 28 Supply Chain Impact Acceleration

As mentioned in Section 4.3.1 there is also future work planned to propose performance and resilience metrics to aid the continuous monitoring of supply chain arrangements and to assist in identifying interventions and improvements, and identify gaps in coverage. Future work is planned to design a selection of appropriate metrics to assess the contribution of each of the four areas in Figure 21 towards improving cybersecurity and resilience of critical national infrastructure. Incentives and resources must be in place to sustain the accountability of actors and achieve agreed goals and responsibilities. Evaluation mechanisms are needed to assess if objectives have been met and to demonstrate the impact of NIS.

This work sets the stage to further build interdisciplinary capability, to enable more resilient solutions for interdependent systems. The contribution of knowledge and experience of establishing and facilitating multi-actor partnerships, and integrating cross-sector perspectives, can be leveraged to build relevant communities and networks for preventing and managing disruptions to infrastructure.

# 10 References


[1] D. Grasso and M. Brown Burkins, *Holistic Engineering Education, Beyond Technology*. New York, NY: Springer New York, 2010. doi: 10.1007/978-1-4419-1393-7.

[2] K. Sayed and H. A. Gabbar, "SCADA and smart energy grid control automation," in *Smart Energy Grid Engineering*, Elsevier, 2017, pp. 481–514. doi: 10.1016/B978-0-12-805343-0.00018-8.

[3] J. Northcote-Green and R. Wilson, *Control and Automation of Electrical Power Distribution Systems*. CRC Press, 2017. doi: 10.1201/9781315221465.

[4] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, "Identifying and Anticipating Cyberattacks That Could Cause Physical Damage to Industrial Control Systems," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 4, pp. 172–182, Dec. 2019, doi: 10.1109/JPETS.2019.2923970.

[5] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[6] M. Jayachandran, Ch. R. Reddy, S. Padmanaban, and A. H. Milyani, "Operational planning steps in smart electric power delivery system," *Sci Rep*, vol. 11, no. 1, p. 17250, Aug. 2021, doi: 10.1038/s41598-021-96769-8.

[7] M. G. Lawrence, S. Williams, P. Nanz, and O. Renn, "Characteristics, potentials, and challenges of transdisciplinary research," *One Earth*, vol. 5, no. 1, pp. 44–61, Jan. 2022, doi: 10.1016/j.oneear.2021.12.010.

[8] J. N. Lieutenant Colonel Rule, "A Symbiotic Relationship: The OODA Loop, Intuition, and Strategic Thought," Philadelphia, 2013.

[9] F. et al Osinga, *Airpower Reborn. The Strategic Concepts of John Warden and John Boyd.* Annapolis: Naval Institute Press, 2015.

[10] N. Mead, *Cyber Security Engineering*. 2017.

[11] K. van der Heijden, *The Sixth Sense, Accelerating Organizational Learning with Scenarios*. 2002.

[12] E. T. Stringer, *Action Research*, 3rd ed. Sage Publications, Inc., 2007.

[13] The European Union Agency for Cybersecurity, “ISAC in a Box,” *ENISA*, 2020. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view (accessed Feb. 14, 2023).

[14] M. G. Burns, “Participatory Operational & Security Assessment on homeland security risks: an empirical research method for improving security beyond the borders through public/private partnerships,” *Journal of Transportation Security*, vol. 11, no. 3–4, pp. 85–100, Dec. 2018, doi: 10.1007/s12198-018-0193-1.

[15] Department for Digital Culture Media and Sport., “The NIS Regulations,” 2018. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018 (accessed Nov. 29, 2022).

[16] European Commission., “NIS Directive,” 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-directive (accessed Nov. 29, 2022).

[17] Department for Digital Culture Media & Sport., “Proposal for legislation to improve the UK’s cyber resilience,” 2022. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience (accessed Nov. 29, 2022).

[18] European Commission., “Proposal for NIS2 Directive,” 2020. https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF (accessed Nov. 29, 2022).

[19] UK Department for Digital Culture Media & Sport., “Consultation outcome: Government response to the call for views on proposals to improve the UK’s cyber resilience,” Nov. 30, 2022. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience (accessed Dec. 05, 2022).

[20] G. HOOGENSEN GJØRV, “Security by any other name: negative security, positive security, and a multi-actor security approach,” *Rev Int Stud*, vol. 38, no. 4, pp. 835–859, Oct. 2012, doi: 10.1017/S0260210511000751.

[21] D. Galafassi *et al.*, “Stories in social-ecological knowledge cocreation,” *Ecology and Society*, vol. 23, no. 1, p. art23, 2018, doi: 10.5751/ES-09932-230123.

[22] J. Anderson, “Researching environmental resistance: working through Secondspace and Thirdspace approaches,” *Qualitative Research*, vol. 2, no. 3, pp. 301–321, Dec. 2002, doi: 10.1177/146879410200200302.

[23] R. Hulme, D. Cracknell, and A. Owens, “Learning in third spaces: developing trans-professional understanding through practitioner enquiry,” *Educ Action Res*, vol. 17, no. 4, pp. 537–550, Dec. 2009, doi: 10.1080/09650790903309391.

[24] C. Otto Scharmer, “Self-transcending knowledge: sensing and organizing around emerging opportunities,” *Journal of Knowledge Management*, vol. 5, no. 2, pp. 137–151, Jun. 2001, doi: 10.1108/13673270110393185.

[25] K. L. Hall, A. L. Vogel, B. A. Stipelman, D. Stokols, G. Morgan, and S. Gehlert, “A four-phase model of transdisciplinary team-based research: goals, team processes, and strategies,” *Transl Behav Med*, vol. 2, no. 4, pp. 415–430, Dec. 2012, doi: 10.1007/s13142-012-0167-y.

[26] W. Hurst, M. Merabti, and P. Fergus, “A Survey of Critical Infrastructure Security,” 2014, pp. 127–138. doi: 10.1007/978-3-662-45355-1_9.

[27] P. Darke, G. Shanks, and M. Broadbent, “Successfully completing case study research: combining rigour, relevance and pragmatism,” *Information Systems Journal*, vol. 8, no. 4, pp. 273–289, Oct. 1998, doi: 10.1046/j.1365-2575.1998.00040.x.

[28] D. Mohajan and H. K. Mohajan, “Constructivist Grounded Theory: A New Research Approach in Social Science,” *Research and Advances in Education*, vol. 1, no. 4, pp. 8–16, Oct. 2022, doi: 10.56397/RAE.2022.10.02.

[29] M. Messenger, “Why would I tell you? Perceived influences for disclosure decisions by senior professionals in inter organisation sharing forums,” Unpublished Masters dissertation, University of London , 2005.

[30] M. Messenger, “Why Would I Tell You? What makes people feel able and motivated to share information?,” Mar. 17, 2010. https://www.enisa.europa.eu/events/information-sharing-workshop/presentations/mandy (accessed Nov. 15, 2022).

[31] H. Borchert, “It Takes Two to Tango: Public-Private Information Management to Advance Critical Infrastructure Protection ,” *European Journal of Risk*

*Regulation* , vol. 6, no. 2, pp. 208–218, 2015, Accessed: Nov. 15, 2022. [Online]. Available: http://www.jstor.org/stable/24769655

[32] W. F. Whyte, *Learning from the Field*. SAGE, 1984.

[33] S. Kumar and R. R. Mallipeddi, "Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions," *Prod Oper Manag*, Oct. 2022, doi: 10.1111/poms.13859.

[34] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: a review and research agenda," *Supply Chain Management: An International Journal*, vol. 25, no. 2, pp. 223–240, Nov. 2019, doi: 10.1108/SCM-10-2018-0357.

[35] S. A. Melnyk, T. Schoenherr, C. Speier-Pero, C. Peters, J. F. Chang, and D. Friday, "New challenges in supply chain management: cybersecurity across the supply chain," *Int J Prod Res*, vol. 60, no. 1, pp. 162–183, Jan. 2022, doi: 10.1080/00207543.2021.1984606.

[36] A. Shaked, L. Tabansky, and Y. Reich, "Incorporating Systems Thinking Into a Cyber Resilience Maturity Model," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 110–115, Jun. 2021, doi: 10.1109/EMR.2020.3046533.

[37] W. Kröger, "Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools," *Reliab Eng Syst Saf*, vol. 93, no. 12, pp. 1781–1787, Dec. 2008, doi: 10.1016/j.ress.2008.03.005.

[38] M. Sitton and Y. Reich, "Enterprise Systems Engineering for Better Operational Interoperability," *Systems Engineering*, vol. 18, no. 6, pp. 625–638, Nov. 2015, doi: 10.1002/sys.21331.

[39] M. & Tritschler, "UK Smart Grid Cyber Security," *Energy Networks Association*, 2011.

[40] E. Drayer, J. Hegemann, S. Gehler, and M. Braun, "Resilient Distribution Grids - Cyber Threat Scenarios and Test Environment," 2016.

[41] Committee on Enhancing the Robustness, R. of Future Electrical Transmission, and D. in the United States to, *Terrorism and the Electric Power Delivery System*. National Academy of Sciences, 2012. doi: 10.17226/12050.

[42] Ofgem, “Investigation into 9 August 2019 power outage,” Aug. 20, 2019. https://www.ofgem.gov.uk/publications/investigation-9-august-2019-power-outage (accessed Feb. 15, 2023).

[43] M. N. Albasrawi, N. Jarus, K. A. Joshi, and S. S. Sarvestani, “Analysis of reliability and resilience for smart grids,” *Proceedings - International Computer Software and Applications Conference*, pp. 529–534, 2014, doi: 10.1109/COMPSAC.2014.75.

[44] M. Fabro, T. Roxey, and M. Assante, “No grid left behind,” *IEEE Secur Priv*, vol. 8, no. 1, pp. 72–76, 2010, doi: 10.1109/MSP.2010.43.

[45] K. Marr, “Electricity security of supply - A commentary on National Grid ’ s Future Energy Scenarios for the next three winters,” *Ofgem, Uk*, pp. 1–24, 2015.

[46] S. Hesmondhalgh, “Approaches to setting electric distribution reliability standards and outcomes,” no. January, pp. 1–191, 2012.

[47] M. Baker, “Shingo Model,” in *WCOM (World Class Operations Management)*, Cham: Springer International Publishing, 2016, pp. 217–226. doi: 10.1007/978-3-319-30105-1_19.

[48] J. von Appen, M. Braun, T. Stetz, K. Diwold, and D. Geibel, “Time in the Sun. The Challenge of High PV Penetration in the German Electric Grid,” *IEEE Power & Energy Magazine*, no. February, pp. 55–64, 2013, doi: 10.1109/MPE.2012.2234407.

[49] O. J. D. Pearce, T. W. Broyd, and N. J. a Murry, “Halstar: systems engineering for sustainable development,” *Proceedings of the ICE - Engineering Sustainability*, vol. 165, pp. 129–140, 2012, doi: 10.1680/ensu.9.00064.

[50] M. Assante, T. Roxey, and A. Bochman, “The Case for Simplicity in Energy Infrastructure For Economic and National Security,” no. October, 2015.

[51] CGI UK, “Cyber security in the boardroom: UK plc at risk,” 2016. Accessed: Feb. 15, 2023. [Online]. Available: https://www.cgi.com/uk/en-gb/article/cgi-cyber-security-research

[52] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the Ukrainian power grid,” *SANS Industrial Control Systems*, p. 23, 2016, [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[53] B. Sobczak and P. Behr, “Inside the Ukrainian hack that put U.S. grid on high alert,” Jul. 18, 2016. https://www.eenews.net/articles/inside-the-ukrainian-hack-that-put-u-s-grid-on-high-alert/ (accessed Feb. 15, 2023).

[54] A. Sternstein, “DHS: Cyberattack on the Ukraine Power Grid Could Happen Here,” Apr. 06, 2016. https://www.nextgov.com/cybersecurity/2016/04/dhs-ukraine-cyberattack-power-grid-could-happen-here/127262/ (accessed Feb. 15, 2023).

[55] M. McElfresh, “Cyberattack on Ukraine grid: here’s how it worked and perhaps why it was done,” Jan. 18, 2016. https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802 (accessed Feb. 15, 2023).

[56] P. Behr and B. Sobczak, “Utilities look back to the future for hands-on cyber defense,” Jul. 21, 2016. https://www.eenews.net/articles/utilities-look-back-to-the-future-for-hands-on-cyberdefense/ (accessed Feb. 15, 2023).

[57] Andrew A Bochman and Sarah Freeman, *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE)*. CRC Press, 2021.

[58] T. Wallis, C. Johnson, and M. Khamis, “Interorganizational Cooperation in Supply Chain Cybersecurity: A Cross-Industry Study of the Effectiveness of the UK Implementation of the NIS Directive,” *Information & Security: An International Journal*, vol. 48, pp. 36–68, 2021, doi: 10.11610/isij.4812.

[59] NCSC, “The principles of supply chain security,” 2018. https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

[60] P. V. ROSENAU, “Introduction:The Strengths and Weaknesses of Public-Private Policy Partnerships,” *American Behavioral Scientist*, vol. 43, no. 1, pp. 10–34, Sep. 1999, doi: 10.1177/0002764299043001002.

[61] M. Dunn-Cavelty and M. Suter, “Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 179–187, 2009, doi: 10.1016/j.ijcip.2009.08.006.

[62] NCSC, “The Cyber Assessment Framework (CAF),” 2019, [Online]. Available: http://dwi.defra.gov.uk/nis/caf/index.html

[63] International Society of Automation, “ISA Standards.” https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/

[64] R. Bradfield, J. Derbyshire, and G. Wright, “The critical role of history in scenario thinking: Augmenting causal analysis within the intuitive logics scenario development methodology,” *Futures*, vol. 77, pp. 56–66, 2016, doi: 10.1016/j.futures.2016.02.002.

[65] National Grid, “Future Energy Scenarios,” 2021. Accessed: Feb. 15, 2023. [Online]. Available: https://www.nationalgrideso.com/news/introducing-our-2021-future-energy-scenarios

[66] A. Bochman, *The End of Cybersecurity*. 2018. Accessed: Feb. 15, 2023. [Online]. Available: https://store.hbr.org/search.php?search_query=Andy%20Bochman&section=product

[67] National Grid ESO, “Bridging the gap to net zero,” 2021. Accessed: Feb. 15, 2023. [Online]. Available: https://www.nationalgrideso.com/future-energy/future-energy-scenarios/bridging-the-gap-to-net-zero

[68] Energy Networks Association, “Distributed Energy Resources – Cyber Security Connection Guidance,” 2020. Accessed: Feb. 15, 2023. [Online]. Available: https://www.energynetworks.org/industry-hub/resource-library/distributed-energy-resources-(der)-cyber-security-connection-guidance.pdf&sa=U

[69] Industrial Internet Consortium, “Industrial Internet Reference Architecture,” pp. 1–101, 2015.

[70] Smart Grid Task Force EG2, “Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems,” 2018.

[71] ENA, “Open Networks Future Worlds,” no. July, 2018, [Online]. Available: http://www.energynetworks.org/electricity/futures/open-networks-project/future-worlds/future-worlds-consultation.html

[72] U.S. Department of Energy, “Electricity subsector cybersecurity capability maturity model (ES-C2M2),” no. February, p. 89, 2014, [Online]. Available: http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

[73] J. H. Allen, P. D. Curtis, and L. P. Gates, “Using Defined Processes as a Context for Resilience Measures,” *Cmu/Sei-2011-Tn-029*, no. December, pp. 246, x, 2011, [Online]. Available: Caralli,

[74] M. Carr, “Public-private partnerships in national cyber-security strategies,” *Int Aff*, vol. 92, no. 1, 2016, doi: 10.1111/1468-2346.12504.

[75] A. Bendiek, R. Bossong, and M. Schulze, “The EU’s Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges.,” *German Institute for International and Security Affairs*, Accessed: Feb. 15, 2023. [Online]. Available: https://www.swp-berlin.org/en/publication/revised-cybersecurity-strategy/

[76] S. L. David and B. Endicott-Popovsky, “Security Beyond Secrecy,” 2017, pp. 305–323. doi: 10.1007/978-3-319-58509-3_25.

[77] K. K. Christensen and K. L. Petersen, “Public–private partnerships on cyber security: a practice of loyalty,” *Int Aff*, vol. 93, no. 6, pp. 1435–1452, Nov. 2017, doi: 10.1093/ia/iix189.

[78] K. Bäckstrand, “Multi-stakeholder partnerships for sustainable development: rethinking legitimacy, accountability and effectiveness,” *European Environment*, vol. 16, no. 5, pp. 290–306, Sep. 2006, doi: 10.1002/eet.425.

[79] R. S. Swarz and J. K. DeRosa, “A Framework for Enterprise Systems Engineering Processes,” pp. 1–10, 2006.

[80] K. E. Eichensehr, “Public-private cybersecurity,” *Tex. L. Rev*, vol. 95, p. 467, 2016.

[81] M. He, L. Devine, and J. Zhuang, “Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach,” *Risk Analysis*, vol. 38, no. 2, pp. 215–225, Feb. 2018, doi: 10.1111/risa.12878.

[82] High Representative of the EU for Foreign Affairs and Security Policy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” 2013. Accessed: Feb. 04, 2022. [Online]. Available:

https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[83] R. Leszczyna, T. Wallis, and M. R. Wróbel, “Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre,” *Decis Support Syst*, vol. 122, no. May, p. 113067, 2019, doi: 10.1016/j.dss.2019.05.007.

[84] V. Bitzer, M. Francken, and P. Glasbergen, “Intersectoral partnerships for a sustainable coffee chain: Really addressing sustainability or just picking (coffee) cherries?,” *Global Environmental Change*, vol. 18, no. 2, pp. 271–284, May 2008, doi: 10.1016/j.gloenvcha.2008.01.002.

[85] J. Meadowcroft, “Democracy and accountability: the challenge for cross-sectoral partnerships,” in *Partenrships, Governance and Sustainable Development: Reflections on Theory and Practice*, Edward Elgar Publishing Ltd, 2007, pp. 194–213.

[86] P. Smith, T. Wallis, and et al, “Cyber Security Incident Response,” 2020. Accessed: Feb. 04, 2022. [Online]. Available: https://www.ee-isac.eu/impact/#

[87] Innovation and Networks Executive Agency, “2020 CEF Telecom Call - Cybersecurity (CEF-TC-2020-2).” Accessed: Feb. 04, 2022. [Online]. Available: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

[88] R. Leszczyna, T. Wallis, and M. R. Wróbel, “Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre,” *Decis Support Syst*, 2019, doi: 10.1016/j.dss.2019.05.007.

[89] A. Harsch, Kulicke M, and et al, “Threat Intelligence Management,” 2020. Accessed: Feb. 04, 2022. [Online]. Available: https://www.ee-isac.eu/impact/#

[90] M. Rocca, S. Schauer, P. Smith, and R. Wolthuis, “Cyber Security Risk Management for Digitalized Energy Systems: Challenges & Solutions,” 2018. Accessed: Feb. 04, 2022. [Online]. Available: https://www.ee-isac.eu/impact/#

[91] R. Leszczyna, T. Wallis, and M. R. Wróbel, “Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre,” *Decis Support Syst*, vol. 122, p. 113067, Jul. 2019, doi: 10.1016/j.dss.2019.05.007.

[92] Electric Power Research Institute, “Cyber Security Metrics for the Electric Sector: Volume 4,” 2018. Accessed: Feb. 20, 2023. [Online]. Available: https://www.epri.com/research/products/000000003002013690

[93] Cybersecurity & Infrastructure Security Agency (CISA), “Traffic Light Protocol (TLP) Definitions and Usage.” https://www.cisa.gov/tlp (accessed Feb. 20, 2023).

[94] J. L. Hernandez-Ardieta, J. E. Tapiador, and G. Suarez-Tangil, “Information sharing models for cooperative cyber defence,” in *5th International Conference on Cyber Conflict (CYCON 2013)*, 2013, pp. 1–28.

[95] 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,” 2020. Accessed: Feb. 04, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0823&from=EN

[96] R. Juriado and N. Gustafsson, “Emergent communities of practice in temporary inter-organisational partnerships,” *The Learning Organisation*, vol. 14, no. 1, pp. 50–61, 2007, Accessed: Feb. 04, 2022. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/09696470710718348/full/html.

[97] P. R. J. Trim and Y.-I. Lee, “The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement,” *Big Data and Cognitive Computing*, vol. 5, no. 3, p. 32, Jul. 2021, doi: 10.3390/bdcc5030032.

[98] M. C. Krutwig and A. Tanțău, “Obligatory versus voluntary energy audits: are there differences in quality?,” *Proceedings of the International Conference on Business Excellence*, vol. 12, no. 1, pp. 522–532, May 2018, doi: 10.2478/picbe-2018-0047.

[99] C. Streck, “New Partnerships in Global Environmental Policy: The Clean Development Mechanism,” *J Environ Dev*, vol. 13, no. 3, pp. 295–322, Sep. 2004, doi: 10.1177/1070496504268696.

[100] C. Nolan, G. Lawyer, and R. M. Dodd, “Cybersecurity: today’s most pressing governance issue,” *Journal of Cyber Policy*, vol. 4, no. 3, pp. 425–441, Sep. 2019, doi: 10.1080/23738871.2019.1673458.

[101] J. Pöyhönen, V. Nuojua, M. Lehto, and J. Rajamäki, “Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations,” *Information & Security: An International Journal*, vol. 43, no. 2, pp. 236–256, 2019, doi: 10.11610/isij.4318.

[102] ENTSO-E / EDSO, “Recommendations for the EC on a Network Code on Cybersecurity,” 2021. Accessed: Feb. 04, 2022. [Online]. Available: https://www.entsoe.eu/network_codes/nccs/#:~:text=The%20Network%20Code%20on%20Cybersecurity%20aims%20to%20set,products%20and%20services%2C%20monitoring%2C%20reporting%20and%20crisis%20management.

[103] A. Barrinha and H. Farrand-Carrapico, “How coherent is EU cybersecurity policy?,” 2018. https://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/ (accessed Feb. 20, 2023).

[104] P. Mee and C. Chandrasekhar, “Cybersecurity is too big a job for governments or business to handle alone,” *World Economic Forum*, May 03, 2021. https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/ (accessed Feb. 20, 2023).

[105] EE-ISAC, “Consultation Questionnaire on the Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows,” 2021. Accessed: Feb. 04, 2022. [Online]. Available: https://documents.acer.europa.eu/Official_documents/Public_consultations/PC_2021_E_04_Responses/EE-ISAC.pdf

[106] ACER EU Agency for the Cooperation of Energy Regulators, “Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows,” Jul. 2021. Accessed: Mar. 04, 2022. [Online]. Available: https://documents.acer.europa.eu/Official_documents/Acts_of_the_Agency/Framework_Guidelines/Framework%20Guidelines/Framework%20Guideline%20on%20Sector-

Specific%20Rules%20for%20Cybersecurity%20Aspects%20of%20Cross-Border%20Electricity%20Flows_210722.pdf

[107] ENTSO-E & E.DSO, “Recommendations for the European Commissionon on a Network Code on cybersecurity,” Feb. 2021. Accessed: Feb. 17, 2023. [Online]. Available: https://energy.ec.europa.eu/system/files/2021-04/nccs_report_network_code_on_cybersecurity_0.pdf

[108] R. Baldwin, M. Cave, and M. Lodge, *Understanding Regulation: Theory, Strategy and Practice*. Oxford University Press, 2012.

[109] UK National Cyber Security Centre, “CISP - Cyber Security Information Sharing Partnership.” https://www.ncsc.gov.uk/section/keep-up-to-date/cisp (accessed Feb. 20, 2023).

[110] Cybersecurity & Infrastructure Security Agency (CISA), “Cyber Information Sharing and Collaboration Program (CISCP).” https://www.cisa.gov/ciscp (accessed Feb. 20, 2023).

[111] Europol, “No More Ransom.” https://www.nomoreransom.org/en/index.html (accessed Feb. 20, 2023).

[112] European Commission, “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,” 2016. Accessed: Feb. 20, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[113] NCSC, “NIS Guidance Collection V1.0,” May 2018.

[114] NCSC, “NCSC CAF Guidance version 3.1,” *https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework*, Apr. 11, 2022.

[115] Carbon Black, “The Ominous Rise of ‘Island Hopping’ & Counter Incident Response Continues,” Apr. 2019. Accessed: Feb. 20, 2023. [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-ominous-rise-of-island-hopping-and-counter-incident-response-continues.pdf

[116] NCSC UK, “CAF Guidance. A4 Supply Chain,” Sep. 26, 2019. https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-4-supply-chain (accessed Feb. 20, 2023).

[117] L. Urciuoli, T. Männistö, J. Hintsa, and T. Khan, “Supply Chain Cyber Security – Potential Threats,” *Information & Security: An International Journal*, vol. 29, pp. 51–68, 2013, doi: 10.11610/isij.2904.

[118] S. Pandey, R. K. Singh, A. Gunasekaran, and A. Kaushik, “Cyber security risks in globalized supply chains: conceptual framework,” *Journal of Global Operations and Strategic Sourcing*, vol. 13, no. 1, pp. 103–128, 2020, doi: 10.1108/JGOSS-05-2019-0042.

[119] BlueVoyant, “Managing cyber risk across the extended vendor ecosystem,” 2020. Accessed: Feb. 20, 2023. [Online]. Available: https://www.dvvs.co.uk/wp-content/uploads/2020/12/BlueVoyant-Supply-Chain-Cyber-Risk-Global-Report-LRES.pdf

[120] Spadafora A, “Energy giant EDP hit with RagnarLocker ransomware,” Apr. 16, 2020. https://www.techradar.com/news/energy-giant-edp-hit-with-ragnarlocker-ransomware (accessed Feb. 20, 2023).

[121] Malwarebytes LABS, “Honda and Enel impacted by cyber attack suspected to be ransomware,” Jun. 09, 2020. https://www.malwarebytes.com/blog/news/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware (accessed Feb. 20, 2023).

[122] A. Hassanzadeh *et al.*, “A review of cybersecurity incidents in the water sector,” *Journal of Environmental Engineering* , vol. 146, no. 5, 2020.

[123] S. Kardon, “Florida Water Treatment Plant Hit With Cyber Attack,” *Industrial Defender*, Feb. 09, 2021. https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack (accessed Feb. 20, 2023).

[124] B. Willemsen and M. Cadee, “Extending the airport boundary: Connecting physical security and cybersecurity,” *Journal of Airport Management*, vol. 12, no. 3, pp. 236–247, 2018.

[125] C. W. Johnson, “Preparing for cyber-attacks on air traffic management infrastructures: cyber-safety scenario generation,” in *7th IET International*

*Conference on System Safety, incorporating the Cyber Security Conference 2012*, 2012, pp. 13–13. doi: 10.1049/cp.2012.1502.

[126] L. H. Newman, "Russia's FireEye Hack Is a Statement—but Not a Catastrophe," *WIRED*, Dec. 08, 2020. https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/ (accessed Feb. 20, 2023).

[127] E. Kovacs, "SolarWinds Says 18,000 Customers May Have Used Compromised Orion Product," *SecurityWeek*, Dec. 14, 2020. https://www.securityweek.com/solarwinds-says-18000-customers-may-have-used-compromised-product/ (accessed Feb. 20, 2023).

[128] G. Corera and J. Tidy, "US Treasury and commerce department targeted in cyber-attack," Dec. 14, 2020. https://www.bbc.co.uk/news/world-us-canada-55265442 (accessed Feb. 20, 2023).

[129] J. Sattler, "Significant attacks on Microsoft Exchange ProxyLogon detected," *F-Secure*, Mar. 19, 2021. https://blog.f-secure.com/microsoft-exchange-proxylogon/ (accessed Feb. 20, 2023).

[130] F. Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?," Feb. 12, 2020. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed Feb. 20, 2023).

[131] Sonatype, "2020 DevSecOps Community Survey," 2020. https://www.sonatype.com/2020survey (accessed Feb. 20, 2023).

[132] Sonatype, "State of the software supply chain," 2021. https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021 (accessed Feb. 20, 2023).

[133] T. Sobb, B. Turnbull, and N. Moustafa, "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions," *Electronics (Basel)*, vol. 9, no. 11, p. 1864, Nov. 2020, doi: 10.3390/electronics9111864.

[134] S. Eggers, "A novel approach for analyzing the nuclear supply chain cyber-attack surface," *Nuclear Engineering and Technology*, vol. 53, no. 3, pp. 879–887, Mar. 2021, doi: 10.1016/j.net.2020.08.021.

[135] A. Yeboah-Ofori and S. Islam, “Cyber Security Threat Modeling for Supply Chain Organizational Environments,” *Future Internet*, vol. 11, no. 3, p. 63, Mar. 2019, doi: 10.3390/fi11030063.

[136] N. Polatidis, M. Pavlidis, and H. Mouratidis, “Cyber-attack path discovery in a dynamic supply chain maritime risk management system,” *Comput Stand Interfaces*, vol. 56, pp. 74–82, Feb. 2018, doi: 10.1016/j.csi.2017.09.006.

[137] IEC62443-2-4, “Security program requirements for IACS service providers.” Accessed: Feb. 20, 2023. [Online]. Available: https://webstore.iec.ch/preview/info_iec62443-2-4%7Bed1.1%7Den.pdf

[138] ENISA, “Guidelines for securing the internet of things,” 2020. Accessed: Feb. 20, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[139] O. Polischuk, “Ecosystem Platform for the Defence and Security Sector of Ukraine,” *Information & Security: An International Journal*, vol. 45, pp. 7–19, 2020, doi: 10.11610/isij.4501.

[140] G. Penchev and A. Shalamanova, “A Governance Model for an EU Cyber Security Collaborative Network – ECSCON,” *Information & Security: An International Journal*, vol. 46, no. 1, pp. 99–113, 2020, doi: 10.11610/isij.4607.

[141] K. Ignatova and D. Tsonev, “Integration of Information Resources to Ensure Collaboration in Crisis Management,” *Information & Security: An International Journal*, vol. 46, no. 2, pp. 141–152, 2020, doi: 10.11610/isij.4610.

[142] A. Ristaino, “Cybersecurity critical for system reliability,” 2016, Accessed: Feb. 20, 2023. [Online]. Available: https://www.isa.org/intech-home/2016/may-june/features/industrial-automation-cybersecurity-conformity-ass

[143] IET, “Code of Practice: Cyber Security and Safety,” 2021. Accessed: Feb. 20, 2023. [Online]. Available: https://electrical.theiet.org/guidance-codes-of-practice/publications-by-category/cyber-security/code-of-practice-cyber-security-and-safety/

[144] IET, “Code of Practice: Cybersecurity for Ships,” 2017. Accessed: Feb. 20, 2023. [Online]. Available: https://electrical.theiet.org/guidance-codes-of-

practice/publications-by-category/cyber-security/code-of-practice-cyber-security-for-ships/

[145] Ofgem, “Competent Authority Guidance for DGE,” 2018. Accessed: Feb. 20, 2023. [Online]. Available: https://www.ofgem.gov.uk/sites/default/files/2022-04/ofgem_ca_guidance_for_dge_gb_v1.0_final.pdf

[146] I.-L. Wu, C.-H. Chuang, and C.-H. Hsu, “Information sharing and collaborative behaviors in enabling supply chain performance: A social exchange perspective,” *Int J Prod Econ*, vol. 148, pp. 122–132, Feb. 2014, doi: 10.1016/j.ijpe.2013.09.016.

[147] L. M. Ellram, “International Purchasing Alliances: An Empirical Study,” *The International Journal of Logistics Management* , vol. 3, pp. 23–36, 1992.

[148] N. Shin and S. Park, “Supply chain leadership driven strategic resilience capabilities management: A leader-member exchange perspective,” *J Bus Res*, vol. 122, pp. 1–13, Jan. 2021, doi: 10.1016/j.jbusres.2020.08.056.

[149] T. J. Pettit, K. L. Croxton, and J. Fiksel, “The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience,” *Journal of Business Logistics*, vol. 40, no. 1, pp. 56–65, Mar. 2019, doi: 10.1111/jbl.12202.

[150] C. Colicchia, A. Creazza, and D. A. Menachof, “Managing cyber and information risks in supply chains: insights from an exploratory analysis,” *Supply Chain Management: An International Journal*, vol. 24, no. 2, pp. 215–240, Mar. 2019, doi: 10.1108/SCM-09-2017-0289.

[151] T. Y. Choi, K. J. Dooley, and M. Rungtusanatham, “Supply networks and complex adaptive systems: Control versus emergence,” *Journal of Operations Management*, vol. 19, no. 3, pp. 351–366, 2001, doi: 10.1016/S0272-6963(00)00068-1.

[152] A. Davis, “Building Cyber-Resilience into Supply Chains,” *Technology Innovation Management Review*, pp. 19–27, 2015, doi: 10.22215/timreview884.

[153] G. C. Stevens and M. Johnson, “Integrating the Supply Chain … 25 years on,” *International Journal of Physical Distribution & Logistics Management*, vol. 46, no. 1, pp. 19–42, Feb. 2016, doi: 10.1108/IJPDLM-07-2015-0175.

[154] C. Roseira, C. Brito, and S. C. Henneberg, “Managing interdependencies in supplier networks,” *Industrial Marketing Management*, vol. 39, no. 6, pp. 925–935, 2010, doi: 10.1016/j.indmarman.2010.06.012.

[155] C. Keegan, “Cyber security in the supply chain: A perspective from the insurance industry,” *Technovation*, vol. 34, no. 7, pp. 380–381, Jul. 2014, doi: 10.1016/j.technovation.2014.02.002.

[156] DCMS, “Cyber Security Breaches Survey,” 2017. Accessed: Feb. 20, 2023. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

[157] DCMS, “NIS Regulations Impact Assessment,” Apr. 2018. Accessed: Feb. 20, 2023. [Online]. Available: https://www.gov.uk/government/publications/nis-regulations-impact-assessment

[158] DCMS, “Cyber Security Breaches Survey,” Mar. 2020. Accessed: Feb. 20, 2023. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

[159] DCMS, “Call for views on amending the NIS Regulations,” Nov. 2018. Accessed: Feb. 20, 2023. [Online]. Available: https://www.gov.uk/government/publications/call-for-views-on-proposed-amendments-to-the-network-and-information-systems-regulations/call-for-views-on-amending-the-nis-regulations-2018

[160] T. Wallis and C. Johnson, “Implementing the NIS Directive, driving cybersecurity improvements for Essential Services,” in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 2020.

[161] EuroControl, “ATM Cybersecurity Maturity Model,” Oct. 2017. Accessed: Feb. 20, 2023. [Online]. Available: https://www.eurocontrol.int/publication/atm-cybersecurity-maturity-model

[162] Scottish Local Government, “Digital Telecare Security Assessment Scheme.” https://telecare.digitaloffice.scot/initiatives/digital-telecare-security-assessment-scheme-55 (accessed Feb. 20, 2023).

[163] D. dos Santos, “AMNESIA:33 – Foresout Research Labs Finds 33 New Vulnerabilities in Open Source TCP/IP Stacks,” 2021. https://www.forescout.com/blog/amnesia33-forescout-research-labs-finds-33-new-vulnerabilities-in-open-source-tcp-ip-stacks/ (accessed Feb. 15, 2023).

[164] S. Simpson, “An assurance-based approach to minimising risks in the software supply chain,” 2010. Accessed: Feb. 20, 2023. [Online]. Available: https://safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf

[165] R. Walton, “What’s in your software? Federal initiative targets frequently overlooked electric utility vulnerabilities,” Mar. 10, 2021. https://www.utilitydive.com/news/whats-in-your-software-federal-initiative-targets-frequently-overlooked-e/595820/ (accessed Feb. 20, 2023).

[166] UK National Cyber Security Centre., “Supply chain security guidance,” Nov. 16, 2018. https://www.ncsc.gov.uk/collection/supply-chain-security (accessed Dec. 16, 2022).