Postprint of: Leszczyna R., Wallis T., Wróbel M.R., Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre, Decision Support Systems, Vol. 122 (2019), 113067, DOI: 10.1016/j.dss.2019.05.007


# Developing Novel Solutions to Realise the EE-ISAC

Rafał Leszczyna[a,*], Tania Wallis[b], Michał R. Wróbel[a]

[a] *Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland*
[b] *University of Strathclyde, 16 Richmond Street, Glasgow, G1 1XQ, United Kingdom*

## Abstract

For more effective decision making in preparation for and response to cyberevents 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. This paper describes two novel solutions proposed during the formation of the European Energy – Information Sharing & Analysis Centre (EE-ISAC) to build situation awareness and support information sharing. The development of EE-ISAC towards regular information sharing among members is described. This demonstrates the foundations achieved so far upon which a situation awareness network can be built for the energy sector.

*Keywords:* cybersecurity, situation awareness, information sharing, ISAC, critical infrastructures, power systems, energy sector

## 1. Introduction

In the last years a significant extension of the cyberthreat landscape has been observed. Modern, advanced cyberattacks are multi-vectored and multi-staged, often extending over a longer period of time (*advanced persistent threats – APTs*) Tounsi and Rais (2018); Skopik et al. (2016); Chen et al. (2018). Moreover,

*Corresponding author
*Email addresses:* rle@zie.pg.gda.pl (Rafał Leszczyna), tania.wallis@strath.ac.uk (Tania Wallis), wrobel@eti.pg.edu.pl (Michał R. Wróbel)

highly targeted and specialised attacks have been introduced (*targeted attacks*) Sun et al. (2018) that aim at concrete computer systems. These threats can lead to very severe consequences especially in case of critical infrastructures and in particular, the electricity sector, as other infrastructures are completely dependent on it. Unfortunately, with increased reliance on Information and Communication Technologies and wide adoption of commodity ICT solutions, they have become a common attack target Skopik et al. (2016); Jang-Jaccard and Nepal (2014).

To enable prompt and effective response to the attacks new approaches are required that provide multilevel situation awareness, from technical, through operational and tactical, to strategic He et al. (2018); Tounsi and Rais (2018); Skopik et al. (2016); Alcaraz and Lopez (2013). *Situational awareness* (SA) regards a thorough explaration of the overall decision-making context and embraces the time-extended perception of an environment, the comprehension of observations and the projection of their status onto the proximate future Tadda and Salerno (2010); Endsley and Garland (2000); Franke and Brynielsson (2014). The *technical-level* SA is related to technological solutions that enable collecting data related to cybersecurity events from miscellaneous system locations. This information is on a daily basis (*operational-level* SA) analysed by security officers in order to recognise attack attempts or ongoing occurrences and promptly react to them (e.g. by applying appropriate countermeasures or reducing the effects Sawik (2013)). The *tactical-level* SA supports cybersecurity decisions that regard longer periods of time and are mostly related to attack prevention and preparation of appropriate countermeasures Fielder et al. (2016) based on detailed attack descriptions derived from cyberincident data collected in lower SA tiers. *Strategic-level* SA concerns high-level cybersecurity knowledge to be used by decision-makers when developing strategies, policies or regulations. At this level *cybersecurity information sharing* (CIS) plays a pivotal role. It relies on partners exchanging

incident-related data such as the descriptions of experienced disturbances, indicators of compromise, proposed remedies and other security expertise to build preparedness for large-scale incidents and future threats de Fuentes et al. (2017); Skopik et al. (2016); Hernandez-Ardieta et al. (2013). It is particularly relevant to the protection of critical infrastructures, where partnerships between public and private sectors are indispesable for adequately protecting the infrastructures from emerging threats Hernandez-Ardieta et al. (2013).

Contemporarily, Information Sharing and Analysis Centres (ISACs) are the institutions designated to lead sector-specific cyberincident information exchange He et al. (2018). With the aim of improving cybersecurity in independent industry areas, they often interlink the industry and the governmental organisations, forming public-private partnerships. In recent years multiple ISACs have been established, including the European Energy – Information Sharing & Analysis Centre (EE-ISAC), the Electricity Information Sharing and Analysis Center (E-ISAC) or the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). They attract members from utilities, vendors, solution providers, academia and research organisations.

This paper presents two novel solutions proposed during the development of EE-ISAC (`www.ee-isac.eu`) to support its operation, namely a three-tier situation awareness network (SAN) and a dedicated, sectoral cyberincident information sharing platform (ISP). The development was carried out by the European project – DEnSeK (Distributed Energy Security Knowledge). The SAN integrates multiple heterogeneous sensors deployed in miscellaneous system locations, with Security Information and Event Management (SIEM) systems and a specialised dashboard to effectively provide cybersecurity situational awareness. The ISP aims at supporting the exchange of sector-specific cyberincident-related data, including case descriptions, experiences or threat descriptions. The interoperability

of the ISP and the SANs is supported by design – the information shared in the ISP can be directly delivered from the SANs.

In the following sections, after the discussion of the relevant work (see Section 2), the situation awareness network (Section 3) and the information sharing platform (see Section 4) are described. Section 5 is devoted to evaluation of the proposed solutions. It includes an overview of utilised testing metrics and description of testing environments, integrity as well as usability tests. Section 6 describes the realisation of EE-ISAC towards establishing information sharing for the energy sector. Section 7 outlines the next stage of development for EE-ISAC. The paper closes with concluding remarks.

## 2. Related work

The research on information sharing and situational awareness centres around five main domains, namely the economic aspects of information sharing (IS), determinants of IS, data formats, tools supporting and conceptual frameworks.

In the area of economic aspects of cybersecurity information sharing (CIS), Gordon et al. Gordon et al. (2003) investigated the impact of IS on security investments and analysed the incentives for information exchange based on economic models. Gal-Or and Ghose Gal-Or and Chose (2005) and Hausken Hausken (2007) complemented this research by applying game-theoretical approaches. The relationships between IS decisions and cybersecurity investments were investigated by Liu et al. Liu et al. (2011). The work of Tosh et al. Tosh et al. (2018) is one of the most recent economic studies on CIS. The authors model the problem area as an evolutionary game between organisations and analyse IS advantages.

In relation to IS determinants and attributes, Vakilinia and Sengupta Vakilinia and Sengupta (2017) studied incentives to share sensitive cyberincident data, with particular consideration to rewarding and participation-fee allocation mechanisms. Analogous, participation cost-related factors were investigated by Tosh

et al. Tosh et al. (2015). Ghose et al. Ghose and Hausken (2015) modelled relationships between attackers carrying out an attack against an enterprise to investigate the incentives for and the optimal level of sharing the information about the company's vulnerabilities. Nikoofal and Zhuang Nikoofal and Zhuang (2015), Zhuang et al. Zhuang et al. (2010), Zhuang and Bier Zhuang and Bier (2010), and Dighe et al. Dighe et al. (2009) applied game theory to determine the role of CIS in cyberdefence strategies. Another approach was adopted by Sedenberg et al. Sedenberg and Mulligan (2015) who analysed public healthcare as a model that enabled identifying guiding principles for cybersecurity information sharing. The principles encompassed governance, reporting, anonymisation, and use limitations.

Over the last decade, several data specifications and standards have been developed to facilitate effective exchange of cybersecurity information. The MITRE-moderated, community-driven work on Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX) and Structured Threat Information Expression (STIX) de Fuentes et al. (2017); Impe (2015); Fransen et al. (2015) is particularly influential as many new developments derive from it. An extension to STIX that supports sharing the information about the impact of cyberevents outside an organisation was proposed by Fransen et al. Fransen et al. (2015) who discuss it in the context of operation of the Dutch National Detection Network (NDN). Qamar et al. Qamar et al. (2017) integrated concepts of STIX and CybOX together with the Common Vulnerabilities and Exposures (CVE) notation and a network model into a Web Ontology Language (OWL)-based ontology that enables threat-related specifications, semantic reasoning and contextual analyses. De Fuentes et al. de Fuentes et al. (2017) enhanced STIX with privacy-preserving mechanisms. A detailed overview of existing solutions in this area is provided in the report of ENISA Bourgue et al.

(2013).

Multiple solutions have been proposed to support SA and CIS. Vakilinia Vakilinia et al. (2017) defined an anonymisation mechanism for information exchange that comprises four main components: registration, sharing, dispute and rewarding. Jajodia et al. Jajodia et al. (2011) described Cauldron – a topological vulnerability analysis tool that aims at supporting mission-centric situational awareness. As a promising direction in detecting modern cyberattacks, collaborative intrusion detection (CIDS) has been studied intensively already for more than a decade Locasto et al. (2005). Recent proposals include a privacy-preserving machine-learning based CIDS for vehicular ad hoc networks (VANETs) Zhang and Zhu (2018), a CIDS designed specifically to protect the smart grid Patel et al. (2017), a trust-based clustering solution that supports deploying CIDS in wireless sensor networks (WSN) Abdellatif and Mosbah (2017) or a CIDS for Advanced Metering Infrastructure (AMI) Liu et al. (2015). Several solutions that support situational awareness are described in the edited volume of Jajodia et al. Jajodia et al. (2010).

As far as operational SA or IS architectures are concerned, platforms such as AlienVault Open Threat Exchange (OTX), Malware Information Sharing Project (MISP) or ThreatView's Cyber Threat & Reputation Intelligence have been developed commercially or by community-driven projects. The scientific research has been focusing on conceptual models or methologies of their development, deployment and governance. Examples of such conceptual frameworks include the proposals of the European Control System Security Incident Analysis Network (ECOSSIAN) project ECOSSIAN; Kaufmann et al. (2015), Barth et al. Barth et al. (2012), Klump and Kwiatkowski Klump and Kwiatkowski (2010) or Brunner et al. Brunner et al. (2011), while Alcaraz and Lopez Alcaraz and Lopez (2013) introduced a systematic approach for developing and establishing situa-

tional awareness architectures in the context of critical infrastructure protection.

The analysis reveals that while scientific studies offer many insights into the CIS and SA domains, the prevalence of them are still on a conceptual level. At the same time, commercial or community-driven solutions do not provide sufficient documentation regarding adopted, potentially innovative, mechanisms. Moreover, both scientific and commercial/open-source contributions tend to separately address high-level, strategic (e.g. sectoral) cyberincident information exchange and technical situational awareness. Combining these areas is highly recommended, especially in the context of critical infrastructure protection Alcaraz and Lopez (2013). The solutions described in this paper support such a joint approach.

## 3. Situation awareness network

Situation awareness networks (SANs) are technical architectures designed to provide situation awareness (SA) by combining multiple sensors deployed in various system locations Bolzoni et al. (2016). Conceptually, SANs are direct instantiation of the collaborative security paradigm. They are responsible for the provision of detailed, processed cyberincident information at the technical and operational level. The US E-ISAC utility members have information sharing devices connected to their networks to send encrypted data to the ISAC for analysis. E-ISAC provides alerts on potential malicious activity and mitigation measures back to the participating organisations. The recent partnership established between US E-ISAC and EE-ISAC is encouraging a new operational stage for EE-ISAC to implement a similar capability.

A specialised SAN architecture was designed, which takes advantage of Security Information and Event Management (SIEM) systems as well as diverse types of sensors, including the dedicated to power systems' communication protocols Leszczyna and Wrobel (2015); Bolzoni et al. (2016); Leszczyna et al. (2016a). Data processing techniques, including data correlation (see Section 4.3), are im-

plemented in order to reduce the number of false positives, increase detection efficiency and facilitate the comprehension of reported information by human operators. This in turn, facilitates decision making and fosters faster reaction to threats and incidents. The architecture is described in Section 3.1.

### *3.1. Architecture*

The SAN for the electricity sector represents a three-tiered architecture illustrated in Figure 1 Leszczyna and Wrobel (2015); Bolzoni et al. (2016); Leszczyna et al. (2016a).

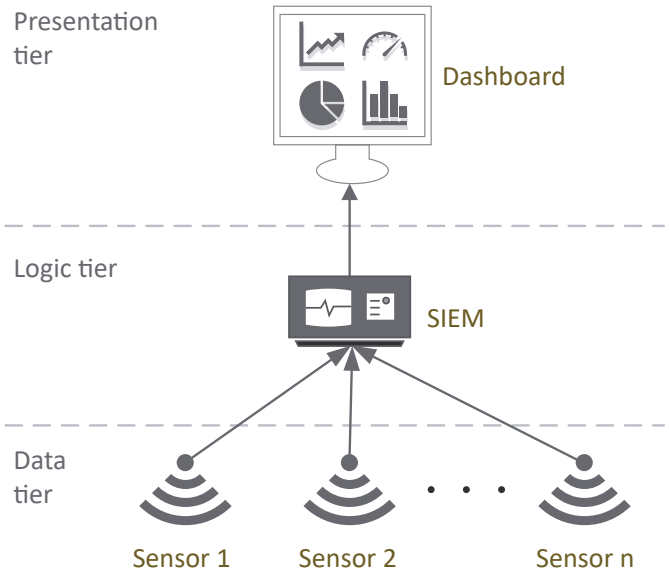


Figure 1: The logical architecture of the cybersecurity situation awareness network for the electricity sector.

The lowest tier – the *data tier* – comprises diverse network and host-based sensors, including different IDS/IPS architectures, network monitoring software and traffic analysis tools, which facilitate system inspection and detection of suspicious events. For instance, a signature-based network intrusion detection system, such as Snort and Suricata, can be applied to detect well-known attack payloads, and several behavioural-based engines to analyse both payloads and flows for anomalies. The need for joining together multiple, heterogeneous sensors stems from

the observation that monitoring tools became specialised and currently they focus on specific threat vectors and analysis approaches. Thus to assure a broader overview of system situation, multiple alternative monitoring techniques need to be applied.

The middle tier of the architecture – the *logic tier* – is dedicated to the Security Information and Event Management (SIEM) system. The SIEM aggregates data from sensors, pre-processes them and transfers to the presentation layer. The sensor data are provided in the `syslog` format. An openly available implementation of a SIEM for industrial environments was a preferable option for application in the power systems SAN. The Bro Network Security Monitor is a network analysis framework which satisfies this criterion. Not constrained to a particular type of detection, it enables implementing proprietary algorithms on the top of its protocol parsers Varadarajan (2012).

The top tier – the *presentation tier* – corresponds to visualisation of the overall system cybersecurity status, which is crucial to attain situational awareness Franke and Brynielsson (2014). The data obtained from the logic tier are further processed and posted on a dedicated dashboard. The dashboard utilises multiple, flexibly configurable visualisation components that enable monitoring diverse aspects of system security situation. The additional tier that enhances the presentation capabilities of SIEM systems was introduced to support recognising the anomalies undetectable to automatic systems due to their mode of operation or particular configuration. The dashboard fosters analysing and filtering large amounts of data to concentrate on the most critical determinants of a cyberincident. It enables observing the evolution of system situation after an event is reported, to thoroughly analyse its nature and to confirm or deny the existence of a threat.

### *3.2. Security requirements for sensors*

The security requirements for the SAN sensors were selected based on the National Information Assurance Partnership (NIAP) protection profiles for intrusion detection systems, sensors, scanners and analysers, published by the U. S. National Security Agency Science Applications International Corporation (2002, 2005c,b,a). The Protection Profiles (PPs) are compliant with Common Criteria. The Common Criteria is an international standard that specifies the criteria for security evaluation of IT hardware and software products (hardware and software) Leszczyna (2018). Sample security objectives for sensors and their supporting environments include auto-protection from unauthorised modifications and access to functions and data, collection and storage of information about all events that may indicate an inappropriate activity, granting authorised users the access only to appropriate functions and data, appropriate handling of potential audit and sensor data storage overflows, ensuring the confidentiality of sensor data when available to other SAN components or secure delivery, installation, management and operation of sensors.

### *3.3. Event correlation rules*

Event correlation rules are machine-readable definitions that allow the SAN finding relations between cybersecurity events, identifying associated events, recognising their common source or target etc., which altogether should facilitate detecting even the most subtle or complex cybersecurity threats.

Rules that introduce prioritisation of SAN alerts were specified to decrease the number of false positives received from the lowest SAN tier, i.e. the data tier. The incident detection rules implemented in the data tier mostly correspond to common industrial automation and control systems (IACS) attack vectors. The highest-priority alerts, which require an immediate response, are raised in the simultaneous occurrence of at least two alerts defined in the correlation table. In

addition, the attack target must be situated in the protected network. In this mode, alerts dispatched by random events are limited, while the overall detection capability remains unaffected. Medium-priority alerts are issued when two alerts of any type are signalled in close time proximity from the data tier. Usually, this corresponds to the situation when an adversary attempts to conduct an automated attack without prior network cognisance. Medium-priority alarms automatically start auto-protection actions, such as IP address blocking. The remaining individual and separate alerts originated from the data tier are assigned the low priority. They are registered in the audit log and can be resolved in a convenient time.

## 4. Information sharing platform

The information sharing platform aims at facilitating the exchange of sector-specific cyberincident-related knowledge by providing communication interfaces and infrastructure. The exchanged information includes extended case descriptions, experiences, detailed processed input from SANs, threat descriptions, countermeasures, good practices, standards and procedures. Based on the input shared between stakeholders, sectoral cybersecurity strategies and policies can be collaboratively developed.

The centralised model of information exchange is implemented, where a central node is introduced which acts as an intermediary in transferring data. The role of the central node plays the information sharing and analysis centre (ISAC). The ISAC-moderated information sharing is promoted in the platform to enable uniform distribution of the information in the whole community, however also peer-to-peer interactions between partners are possible. In addition, the central hub of the ISAC communicates with other ISACs and non-ISAC hubs, exchanging information in various forms such as client and server or hub and spoke. Both, unidirectional and bidirectional communication with the central node is

facilitated, primarily in the asynchronous form. To facilitate the transmission of all cyberincident-related data, both in natural language and machine-readable formats, a dedicated data model was developed, which incorporates established specifications in this area (see Section 4.1).

To encourage sharing delicate information an anonymity architecture has been established (see Section 4.5) and data sanitisation mechanisms (see Section 4.2) have been introduced. The architecture takes advantage of the mobile agents paradigm that is particularly suitable for the deployment in heterogeneous environments, such as the power sector. Data sanitisation, on the other hand enables maintaining a good equilibrium between security and usefulness of exchanged data. Cybersecurity requirements brought out specifically for the power sector's information sharing platform are described in Section 4.4.

### *4.1. Data model*

The crucial element during the development of an information sharing platform is designing a data model. This step is essential to determine the types of data exchanged in the platform, facilitate the communication between the developers of the ISP and its future users, in particular during the elicitation and analysis of software requirements, and support the specification of other functionalities including data sanitisation or aggregation (see Sections 4.2 and 4.3).

The electricity sector exposes specific characteristics that need to be embraced in the model. In particular, the heterogeneity and geographical distribution of participants and automatically generated data should be considered. The future users of the ISP represent diverse domains and sectors, implement various business models and have different (sometimes opposite) interests and forms of activity. In addition, they are situated in dispersed, often remote, geographical locations. As a result, establishing an efficient communication with all participants is hindered, especially in regard to physical meetings-based. Such communication is indis-

pensable for obtaining users' input and feedback regarding the types and format of exchanged data. As far as the second characteristic is concerned, part of the information exchanged in the ISP would be delivered by SANs and security solutions such as IDS/IPS or anti-malware tools. The developed data model needs to encompass the machine-generated contents.

To assure data model compatibility with machine-generated contents, standardised data representations for security information i.e. the Intrusion Detection Message Exchange Format (IDMEF) Debar et al. (2007) and the Incident Object Description and Exchange Format (IODEF) Danyliw et al. (2007), as well as the Dublin Core Metadata ISO (2009) for general purpose documents were integrated into the model. IDMEF specifies formats and procedures for the exchange of information between intrusion detection and response systems as well as management systems that need to interact with them Debar et al. (2007). Almost all popular IDS, including Snort, Suricata or OSSEC enable IDMEF-based communication. IODEF defines a common data format for describing and exchanging information about incidents between Computer Security Incident Response Teams (CSIRTs). It is fully compatible with IDMEF, yet extends it with objects enabling communication between people and teams Danyliw et al. (2007). Dublin Core, standardised as ISO 15836:2009 ISO (2009), specifies a set of fifteen properties for describing resources. It enables detailed descriptions of documents. The approach was applied to create the entire, 3-levelled data model for the cyberincidents information sharing platform for the electricity sector Leszczyna and Wróbel (2014); Leszczyna and Wrobel (2014). Information assets were identified based on the analysis of data which can be created and shared by sectoral stakeholders.

### *4.2. Data sanitisation*

At the stage of detecting a cyberincident, its descriptive data should be as detailed as possible, to enable effective response. For this purpose, the information

about IP addresses, protocols, ports, event timing, sensor identity, and often packet headers or the payload are captured. However, when this data is to be shared on an ISP, the high level of detail in the information may contradict its security. The data are no longer delivered to a trusted and well known system administrator who usually works for the company, but need to be shared with all external participants of the information sharing platform. This creates various opportunities for an attacker to explore and misuse the shared data. In addition, sharing certain details may be undesirable, even in trusted circles.

A technique that enables preserving a balance between security and usefulness of shared data is *data sanitisation*. It aims at preventing information from being used for unintended purposes, which is achieved by removing or altering its sensitive parts. Multiple techniques of data sanitisation exist. For instance, in *generalisation*, data are replaced with a range of possible values that the attribute may assume Bishop et al. (2010), *Bloom filters* are one-way data structures used for sanitising IP addresses that while preventing any data extraction, enable verification if a datum was previously inserted into the filter if presented a second time to the filter Locasto et al. (2005), while *data cubes* hash the addresses of observables to a limited set of coordinates, and represent intensity of observables as two-dimensional values, and time as a third dimension Valdes et al. (2006). Moreover, variants of the methods are often available. Generalisation methods include *suppression* – omitting a sensitive datum Crawford et al. (2007), *deletion* – removing a value Bishop et al. (2010), *aggregation* – categorising a datum with other data Crawford et al. (2007) or *number variance* – modifying each number value by a random percentage of its original value Edgar (2004).

The advantage of data sanitisation techniques is that they do not utilise cryptography and consequently they do not require keys management. This renders them very suitable for the application in energy sectors. There, the key manage-

ment process is very demanding due to the scale and diversity of participating information systems. Sanitisation rules were defined for each entity of the data model described in Section 4.1. Two sanitisation levels were distinguished. The low level of sanitisation refers to the situation where only the most sensitive data are sanitised. High-level sanitisation, on the other hand, aims at protecting also the data which could only potentially provide some indirect indications to an attacker, who based on additional knowledge, could infer the value of critical data. Sample sanitisation rules are presented in Tables 1 and 2

Table 1: Sanitisation rules for the *Method* data model entity.

| Title | Method | | |
|---|---|---|---|
| Description | The entity provides information about the method used by an attacker in form of a reference to a vulnerability or exploit database or a free-form description. | | |
| Field | Description | Sanitisation | |
| | | Low | High |
| Type | Type of the method e.g. DDoS, virus, stack-overflow | No | No |
| Name | Name of the method | No | No |
| Description | Brief description of the method (Full description should be shared as a separate document.) | No | No |

Table 2: Sanitisation rules for the *Attack* data model entity.

| Title | Method | | |
|---|---|---|---|
| Description | The entity contains information about the security events that constitute the incident. | | |
| Field | Description | Sanitisation | |
| | | Low | High |
| Description | The time when the incident activity was first detected by the reporter. In the case of more than one event, the time the first event was detected. | No | Yes |

### *4.3. Data aggregation*

As written in Section 4.1, part of the data exchanged in the information sharing platform are generated automatically by SANs and security solutions such as SIEMs or IDS/IPS. These tools may provide large amounts of redundant information that can be difficult to analyse by human operators. Data correlation and aggregation algorithms help in resolving this issue.

The development of aggregation algorithms includes the selection of grouping attributes i.e. the data entities for which identical or similar values (depending on the selected criteria) in distinct messages would result in aggregating the messages. Examples of grouping attributes include the attack source, the attacked service, the attack method, the attacked application or the attacked operating system. The next step is to map the selected attributes to the appropriate entities in the data model. The aggregation will be possible only if grouping attributes have not been previously sanitised (see Section 4.2). In the algorithms, the maximum time between incidents (MTBI) plays an important role as it is used to determine whether an incident can be treated as part of a previously detected attack. For instance, if set to 1 hour, the information about a DoS attack against the same group of hosts with an interval larger than 1 hour would be recognised on the ISP platform as two separate incidents. For each grouping attribute, a separate MTBI can be assigned. An example of the aggregation algorithm is presented in Figure 2.

### *4.4. Cybersecurity requirements*

Cybersecurity requirements for the information sharing platform were elicited based on the study that comprised the identification of available security requirements for alternative security ISPs developed for other industries, the review of the literature on security requirements engineering and the analysis of the available sources of security requirements for Content Management Systems (CMSs), web applications and databases – as an ISP is a form of a specialised CMS. As a result security requirements categorised into 15 areas have been identified. The categories include risk assessment, authorisation and access control, cryptography, penetration testing, server and application validation, protection from malicious code or anonymity and data sanitisation. More details on the requirements and their elicitation process can be found in Leszczyna et al. (2016b).

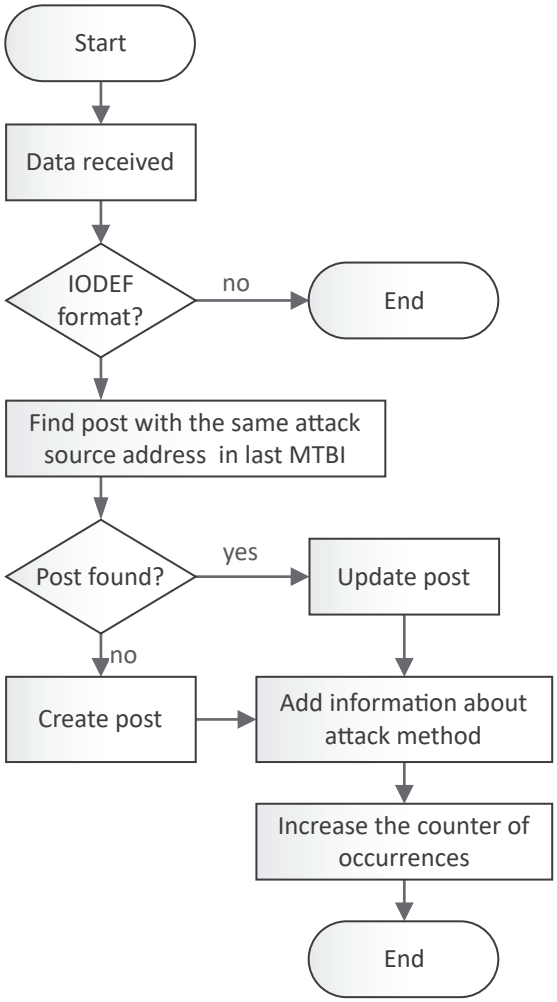


Figure 2: Data aggregation algorithm for the `attack method` data fields. MTBI depicts the maximum time between incidents.

### *4.5. Anonymisation mechanisms*

In addition to data sanitisation (see Section 4.2) which in principle prevents shared data from being used for unintended purposes by obscuring unnecessary details, the mechanisms that enable anonymity of the information senders have been introduced. This to encourage exchange of even highly sensitive information between platform participants with different trust levels. The anonymity mechanisms in the information sharing platform for the electricity sector aim at protecting the identity of information senders by concealing all personally iden-

tifiable information (PII) as well as by mitigating more sophisticated attacker techniques which aim at revealing the target's identity (traffic analysis Leszczyna (2007)).

A mobile agent-based anonymity architecture described in Leszczyna (2007); Leszczyna and Górski (2006, 2005) was adapted to the ISP. The architecture is composed of two modules, namely the *Module I: Untraceability Protocol Infrastructure* and the *Module II: Additional Untraceability Support* (optional). The first module constitutes the core of the architecture. It implements an untraceability protocol to assure that the address of a message sender to the ISP is obfuscated. The second part of the anonymity architecture aims at providing further anonymity protection i.e. the protection against traffic analysis and tracing through reading data held by agents. This module is based on optional components, which implementation and application should be preceded with a thorough requirements analysis and feasibility study as each of the components, while strengthening security of the system, also introduces an (often significant) overhead Leszczyna et al. (2015).

To effectively protect the ISP, the anonymity architecture should be deployed in multiple, dispersed network nodes. In the energy sector, the heterogeneity and geographical distribution of its participants constitutes a strength, that should be taken advantage of at this stage. With the variety of participating stakeholders, organisations, technological solutions and system architectures, the energy sector is a complex environment, in which anonymisation nodes of the anonymity architecture can become practically completely secure from being altogether, or in a large subset, observed by an attacker. The anonymisation nodes can be deployed in offices, power plants, substations. Mobile agents facilitate deployment and communication in such complex and heterogeneous environments Gray et al. (2000).

## 5. Evaluation

The first step of the evaluation of the proposed solutions was related to the design of testing metrics, in order to enable systematic measurements. This was followed by integrity tests that aimed at checking the interoperation of SAN components. To assess the quality of interfaces and human-computer interactions involved in information exchange activities usability tests were performed.

### *5.1. Testing metrics*

Testing metrics enable objective evaluation of products and their development processes. Various types of metrics, including performance, effectiveness or complexity metrics, have been devised for different ICT domains. The cybersecurity SA and ISP areas, however, due to their novelty, required new consideration. When introducing metrics, specific criteria were taken into account. The metrics should enable consistent measuring, need to be expressed as a cardinal number or percentage and represented in units of measure. They must be contextually specific, achievable at a reasonable cost and easily implementable in the SA and ISP context at every stage of development Bolzoni et al. (2016); Leszczyna et al. (2016a).

Three categories of metrics have been proposed: *testing process metrics*, *cybersecurity metrics* and *usability metrics* Bolzoni et al. (2016); Leszczyna et al. (2016a). *Testing process metrics* facilitate the control and management of a testing procedure. The selected metrics include source code coverage, test case defect density, failures detection rate and test improvement in product quality. *Cybersecurity metrics*, derived from the IDS/IPS and SIEM domains, are directly related to SAN operation. They include accuracy, detection rate, false positive rate, mean time between failures and time to protect. *Usability metrics* refer to the usability of ISP tools and are mainly associated with the quality of the ISP interfaces and the human-machine interactions it enables. The selected metrics include task

success, time-on-task, efficiency, errors and learnability. The metrics were applied during the tests described in the next sections.

### *5.2. Testing environment*

The tests were performed mostly in two testing environments. The situation awareness network was tested in the cybersecurity laboratory of the Enel Engineering and Research located in the power plant area of Livorno. This laboratory is designed to replicate operational environments associated with power generation. It is primarily dedicated to testing and development of process control applications and comprises all crucial components of industrial control systems, including PLCs and Distributed Control Systems (DCSs) from various vendors. The laboratory's computer network is layered in the same way as in a production plant. The physical part of this cyber-physical system reproduces the closed water cycle similar to that associated with electric power generation. It is equipped with field devices such as pressure meters, valves, pumps, inverters, etc. controlled by PLCs.

The tests of the information sharing platform, where human interactions are strongly involved, were carried out in the laboratory at Gdańsk University of Technology. The infrastructure utilised in tests consisted of several interconnected desktop computers with JADE agent platform, VirtualBox'es for computer systems emulation, Vagrant development environments management software, Wordpress content management system (CMS) to reflect information sharing activities, Eclipse software development environment, Maven software project management framework that supports project integration and unit testing, and the Git version-control system.

### *5.3. Integrity tests*

Integrity tests aimed at verifying correct interoperation of SAN components. The evaluated SAN architecture consisted of the dashboard (see Section 3.1), a

SIEM (the AlienVault's OSSIM ) and the Argus network analyser together with the Snort Network Intrusion Detection and Prevention System as SAN sensors. In addition, the TCPReplay, Oinkmaster and Barnyard2 open software tools were used to facilitate test performance.

The primary test cases aimed at checking the dashboard operation with the Argus analyser as the data source. During these tests several problems were identified. All of them related to the processing and visualisation of large amount of data specific to the power plant environment. Feedback from testing helped developers to identify and fix bugs.

During the second phase of testing, the integration between Snort IDS and OSSIM SIEM was examined. While, during the deployment and configuration of both systems no issues were encountered, the testing in larger-scale environment revealed problems with communication between subnets. This was a relatively critical issue, as in real production environments sensors will be dispersed across regions and countries, and their stable and secure connection with the SIEM node is indispensable for provising situational awareness.

The last test cases were designed to evaluate the full integration of the SAN. Communication through all tiers of the SAN architecture was tested. The data collected by sensors were delivered to the SIEM system. There, after the application of data processing and analysis algorithms, alerts were raised and the dashboard was notified. The operator was informed about detected threats through the dashboard widgets. During the tests, several minor issues and bugs were identified, however the overall SAN design proved correct.

### *5.4. Usability tests*

Usability tests were performed to evaluate the quality of interfaces and human-computer interactions involved in information sharing activities. To enable relative assessments, anonymity architecture-supported (see Section 4.5) message

sending was compared to the analogous task performed with Tor Browser , which is the most popular anonymisation tool available on the Internet. The tests involved 13 participants. Their usability perceptions were measured using the Likert scale, after the comparative analysis of four software usability metrics, namely the System Usability Scale (SUS), Software Usability Measurement Inventory (SUMI), Computer System Usability Questionnaire (CSUQ) and Website Analysis and MeasureMent Inventory (WAMMI).

Each participant was provided with a description of two tasks, separately for the two interfaces i.e. the anonymity architecture and the ToR browser. The first task regarded the installation of the interface, the second – sending of an anonymous message. After the tasks' completion, users were filling in a questionnaire comprising 14 closed-ended and one open-ended question. The closed-ended questions aimed at determining the level of ease of use, impressions regarding the graphical aspects of the interface and other perceptions, using the Likert scale or yes/no answers. The open question was dedicated to suggestions on the improvement of the interfaces.

The tests showed faster completion of the message sending task using the anonymity architecture. At the same time, the majority of users preferred the ToR browser interface, indicating that it is more 'user-friendly' and 'intuitive'. Consequently, the improvement of the anonymity architecture front-end constitutes a potential subject of further works on the solution.

## 6. Current EE-ISAC activities and tools

The original vision of EE-ISAC was to join forces across the whole energy supply chain and improve awareness among all stakeholders. 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 organ-

isations 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. As a result, close working relations to develop and encourage sharing of sensitive information during EE-ISAC's closed member only meetings have been established.

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 so far with building membership, creating partnerships and forming working groups is concerned, 23 representatives of utilities, vendors, public bodies, academia and research labs have signed the membership, 10 task forces have been established and mutual agreements have been signed with Japan and US E-ISACs.

During the development of EE-ISAC it has been necessary to encourage the participation of utilities to keep EE-ISAC's work and approach always tailored to the needs of energy utilities. Essential topic areas were chosen and several technical working groups were formed to commence specific information sharing activities. This enabled focussed collaborative communities to form within EE-ISAC to work together on the current issues, as demonstrated by Figure 3.

In addition to holding regular member meetings, a digital sharing platform was launched, shown in Figure 4, which takes advantage of the DEnSeK proposals (see Section 4). This is used for posting regular security bulletins and new information on threats and vulnerabilities. It also offers a place for discussion among technical working groups. Members appreciate the added value of EE-ISAC as a forum for discussing relevant topics and issues they all face.

EE-ISAC is forming its own instance of malware information sharing tailored especially for the energy sector (see Figure 5) that implements the concepts de-

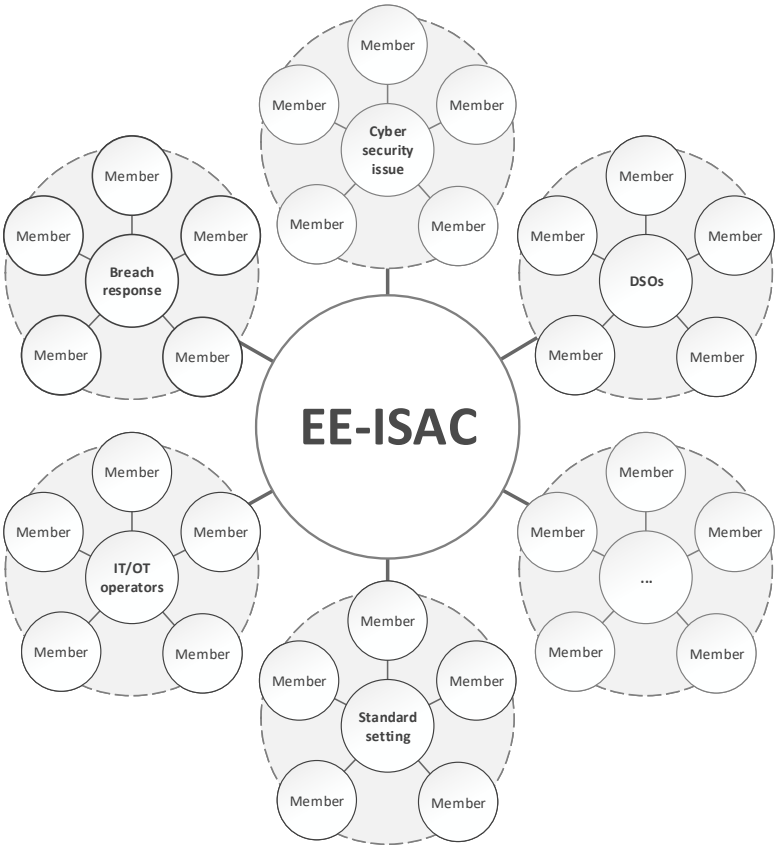


Figure 3: Communities within EE-ISAC

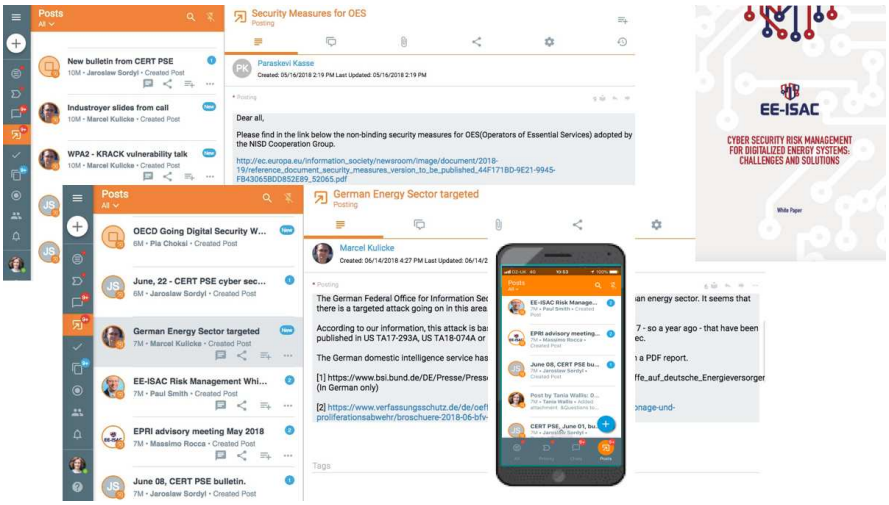


Figure 4: EE-ISAC's information sharing platform at work

scribed in Section 4. This is being progressed by EE-ISAC's threat intelligence working group and will soon become available to all EE-ISAC members to both contribute to content and receive the latest information.

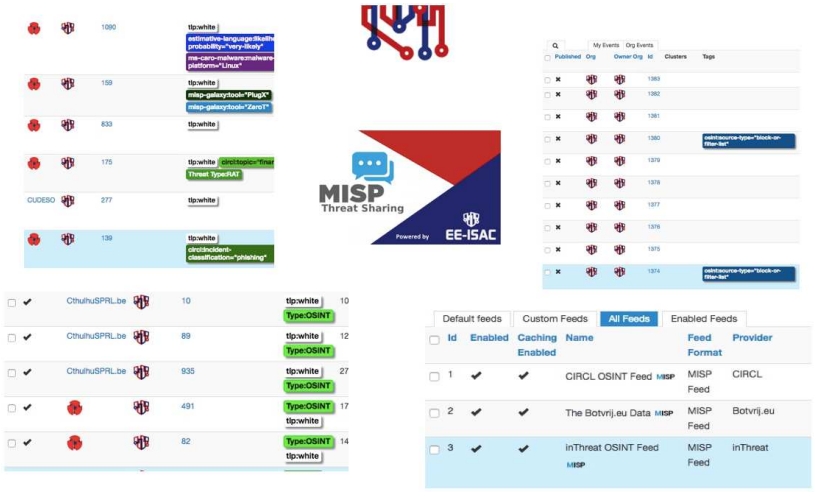


Figure 5: EE-ISAC threat sharing

## 7. Future decision support for EE-ISAC

The next stage of development for EE-ISAC could build the situation awareness network envisioned during the DEnSeK project and described here in Section 3. As well as attending to the cybersecurity needs of utility members, EE-ISAC has recognised the importance of broadening their situation awareness network through developing global partnerships. EE-ISAC's new partnerships within Europe and in USA and Japan offer the chance to work towards a future vision of 24 x 7 decision support across three time zones in USA, Europe and Japan. This opportunity will explore and define appropriate and necessary information sharing and analysis between utilities and between nations for the energy sector. There is also work ongoing to support the cyber security capabilities of smaller utilities, cross-sector collaborations with other ISACs and to encourage the establishment of new energy ISACs in other areas.

## 8. Conclusions

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 have established a vision for the developments within EE-ISAC to work towards. Significant progress has 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.

## 9. Acknowledgements

The study presented in this paper is based on work carried out in the DEnSeK (Distributed Energy Security Knowledge) project founded by the European Commission, Directorate-General for Home Affairs (Programme ,,Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks" – CIPS, Project Reference: HOME/2012/CIPS/AG/4000003772) and partially supported from the project funds. It is also supported by the DS Programs of Faculty of Management and Economics and Faculty of Electronics, Telecommunications and Informatics of Gdańsk University of Technology. EE-ISAC have also supported this paper through their experiences with implementing ISP and SAN.

## References

## References

Abdellatif, T. and Mosbah, M. (2017). Efficient monitoring for intrusion detection in wireless sensor networks. *Concurrency and Computation: Practice and*

*Experience*, page e4907.

Alcaraz, C. and Lopez, J. (2013). Wide-area situational awareness for critical infrastructure protection. *Computer*, 46(4):30–37.

Barth, R., Meyer-Nieberg, S., Pickl, S., Schuler, M., and Wellbrink, J. (2012). A toolbox for operational analysis. In *Emerging M and S Applications in Industry and Academia Symposium 2012, EAIA 2012*, pages 106–113, Orlando, Florida, USA. Society for Computer Simulation International.

Bishop, M., Cummins, J., Peisert, S., Singh, A., Bhumiratana, B., Agarwal, D., Frincke, D., and Hogarth, M. (2010). Relationships and data sanitization: a study in scarlet. In *NSPW '10 Proceedings of the 2010 New Security Paradigms Workshop*, pages 151–164, Concord, Massachusetts, USA. ACM.

Bolzoni, D., Leszczyna, R., Wróbel, M. R., and Wrobel, M. (2016). Situational Awareness Network for the electric power system: The architecture and testing metrics. In Ganzha, M., Maciaszek, L., and Paprzycki, M., editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, FedCSIS 2016*, pages 743–749, Gdansk, Poland. IEEE.

Bourgue, R., Budd, J., Homola, J., Wlasenko, M., and Kulawik, D. (2013). Detect, SHARE, Protect Solutions for Improving Threat Data Exchange among CERTs. Technical Report October.

Brunner, M., Hofinger, H., Roblee, C., Schoo, P., and Todt, S. (2011). Anonymity and privacy in distributed early warning systems. In *Critical Information Infrastructures Security*, volume 6712 LNCS, pages 81–92. Springer, Berlin, Heidelberg.

Chen, J., Su, C., Yeh, K.-H., and Yung, M. (2018). Special Issue on Advanced Persistent Threat. *Future Generation Computer Systems*, 79:243–246.

Crawford, R., Bishop, M., Bhumiratana, B., Clark, L., and Levitt, K. (2007). Sanitization models and their limitations. In *Schloss Dagstuhl, Germany*, pages 41–56, Schloss Dagstuhl, Germany. ACM.

Danyliw, R., Meijer, J., and Demchenko, Y. (2007). RFC 5070 - The Incident Object Description Exchange Format (IODEF).

de Fuentes, J. M., González-Manzano, L., Tapiador, J., and Peris-Lopez, P. (2017). PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers and Security*, 69:127–141.

Debar, H., Curry, D., and Feinstein, B. (2007). RFC 4765 - The intrusion detection message exchange format (IDMEF).

Dighe, N. S., Zhuang, J., and Bier, V. M. (2009). Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence. *International Journal of Performability Engineering*, 5(1):31–43.

ECOSSIAN. European COntrol System Security Incident Analysis Network (ECOSSIAN) Project Website.

Edgar, D. (2004). Data Sanitization Techniques. Technical report, Net 2000.

Endsley, M. R. and Garland, D. J. (2000). *Situation Awareness Analysis and Measurement*. CRC Press, Inc.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., and Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86:13–23.

Franke, U. and Brynielsson, J. (2014). Cyber situational awareness - A systematic review of the literature. *Computers and Security*, 46:18–31.

Fransen, F., Smulders, A., and Kerkdijk, R. (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *e & i Elektrotechnik und Informationstechnik*, 132(2):106–112.

Gal-Or, E. and Chose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2):186–208.

Ghose, A. and Hausken, K. (2015). A Strategic Analysis of Information Sharing Among Cyber Attackers. *Journal of Information Systems and Technology Management*, 12(2):245–270.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6):461–485.

Gray, R. S., Kotz, D., Cybenko, G., and Rus, D. (2000). Mobile Agents: Motivations and State-of-the-Art Systems. Technical Report TR2000-365, Dartmouth College, Hanover, NH.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6):639–688.

He, M., Devine, L., and Zhuang, J. (2018). Perspectives on Cybersecurity Information Sharing among Multiple Stakeholders Using a Decision-Theoretic Approach. *Risk Analysis*, 38(2):215–225.

Hernandez-Ardieta, J. L., Suarez-Tangil, G., and Tapiador, J. E. (2013). Information Sharing Models for Cooperative Cyber Defence. In *2013 5th International Conference on Cyber Conflict*, pages 60– 87, Tallinn, Estonia.

Impe, K. V. (2015). How STIX, TAXII and CybOX Can Help With Standardizing Threat Information.

ISO (2009). ISO 15836:2009 - Information and documentation - The Dublin Core metadata element set.

Jajodia, S., Liu, P., Swarup, V., and Wang, C. (2010). *Cyber situational awareness: advances in information security*. Springer, Berlin.

Jajodia, S., Noel, S., Kalapa, P., Albanese, M., and Williams, J. (2011). Cauldron: Mission-centric cyber situational awareness with defense in depth. In *Proceedings - IEEE Military Communications Conference MILCOM*, pages 1339–1344, Baltimore, MD, USA. IEEE.

Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5):973–993.

Kaufmann, H., Hutter, R., Skopik, F., and Mantere, M. (2015). A structural design for a pan-European early warning system for critical infrastructures. *e & i Elektrotechnik und Informationstechnik*, 132(2):117–121.

Klump, R. and Kwiatkowski, M. (2010). Distributed IP watchlist generation for intrusion detection in the electrical smart grid. *IFIP Advances in Information and Communication Technology*, 342 AICT:113–126.

Leszczyna, R. (2007). Anonymity Architecture for Mobile Agent Systems. In Ma\v rík, V., Vyatkin, V., and Colombo, A. W., editors, *Holonic and Multi-Agent Systems for Manufacturing*, volume 4659 of *Lecture Notes in Computer Science*, pages 93–103. Springer Berlin Heidelberg, Heidelberg, Germany.

Leszczyna, R. (2018). Standards on Cyber Security Assessment of Smart Grid. *International Journal of Critical Infrastructure Protection*, 22:70–89.

Leszczyna, R. and Górski, J. (2006). An Untraceability Protocol for Mobile Agents

and Its Enhanced Security Study. In *15th EICAR Annual Conference Proceedings*, pages 26–37, Hamburg, Germany.

Leszczyna, R., Łosiński, M., and Małkowski, R. (2015). Security Information Sharing for the Polish Power System. In *Proceedings of the Modern Electric Power Systems 2015 - MEPS 2015*, pages 163 – 169, Wroclaw, Poland. IEEE.

Leszczyna, R., Małkowski, R., and Wróbel, M. R. (2016a). Testing Situation Awareness Network for the Electrical Power Infrastructure. *Acta Energetica*, 3(28):81–87.

Leszczyna, R. and Wróbel, M. R. (2014). Data Model Development for Security Information Sharing in Smart Grids. *International Journal for Information Security Research*, 4:479–489.

Leszczyna, R. and Wrobel, M. R. (2014). Security information sharing for smart grids: Developing the right data model. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pages 163–169, London, UK. IEEE.

Leszczyna, R. and Wrobel, M. R. (2015). Evaluation of open source SIEM for situation awareness platform in the smart grid environment. In *2015 IEEE World Conference on Factory Communication Systems (WFCS)*, pages 1–4, Palma de Mallorca, Spain. IEEE.

Leszczyna, R., Wrobel, M. R. M., and Malkowski, R. (2016b). Security requirements and controls for incident information sharing in the polish power system. In *Proceedings - 2016 10th International Conference on Compatibility, Power Electronics and Power Engineering, CPE-POWERENG 2016*, pages 94–99, Bydgoszcz, Poland. IEEE.

Leszczyna, R. R. and Górski, J. (2005). Untraceability of mobile agents. In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems - AAMAS '05*, volume 3, page 1233, Utrecht, the Netherlands. ACM.

Liu, D., Ji, Y., and Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems*, 52(1):95–107.

Liu, X., Zhu, P., Zhang, Y., and Chen, K. (2015). A Collaborative Intrusion Detection Mechanism Against False Data Injection Attack in Advanced Metering Infrastructure. *IEEE Transactions on Smart Grid*, 6(5):2435–2443.

Locasto, M. E., Parekh, J. J., Keromytis, A. D., and Stolfo, S. J. (2005). Towards collaborative security and P2P intrusion detection. In *Proceedings from the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop, SMC 2005*, volume 2005, pages 333–339, West Point, NY, USA. IEEE.

Nikoofal, M. E. and Zhuang, J. (2015). On the value of exposure and secrecy of defense system: First-mover advantage vs. robustness. *European Journal of Operational Research*, 246(1):320–330.

Patel, A., Alhussian, H., Pedersen, J. M., Bounabat, B., Júnior, J. C., and Katsikas, S. (2017). A nifty collaborative intrusion detection and prevention architecture for Smart Grid ecosystems. *Computers and Security*, 64:92–109.

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., and Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers and Security*, 67:35–58.

Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55(1):156–164.

Science Applications International Corporation (2002). Intrusion Detection System System Protection Profile Version 1.4. Technical report, National Security Agency.

Science Applications International Corporation (2005a). Intrusion Detection System Analyzer Protection Profile Version 1.2. Technical report, National Security Agency, Columbia,.

Science Applications International Corporation (2005b). Intrusion Detection System Scanner Protection Profile Version 1.2. Technical report, National Security Agency, Columbia,.

Science Applications International Corporation (2005c). Intrusion Detection System Sensor Protection Profile Version 1.2. Technical report, National Security Agency, Columbia,.

Sedenberg, E. M. and Mulligan, D. K. (2015). Public health as a model for cybersecurity information sharing. *Berkeley Technology Law Journal*.

Skopik, F., Settanni, G., and Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, 60:154–176.

Sun, C.-C., Hahn, A., and Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56.

Tadda, G. P. and Salerno, J. S. (2010). Overview of Cyber Situational Awareness. In Jajodia, S., Liu, P., Swarup, V., and Wang, C., editors, *Cyber Situational Awareness*, volume 46 of *Advances in Information Security*, pages 15–35. Springer US, Boston, MA.

Tosh, D., Sengupta, S., Kamhoua, C., Kwiat, K., and Martin, A. (2015). An evolutionary game-theoretic framework for cyber-threat information sharing. In *IEEE International Conference on Communications*, pages 7341–7346, London, UK. IEEE.

Tosh, D., Sengupta, S., Kamhoua, C. A., and Kwiat, K. A. (2018). Establishing evolutionary game models for CYBer security information EXchange (CYBEX). *Journal of Computer and System Sciences*, 98(July 2016):27–52.

Tounsi, W. and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security*, 72:212–233.

Vakilinia, I. and Sengupta, S. (2017). A coalitional game theory approach for cybersecurity information sharing. In *Proceedings - IEEE Military Communications Conference MILCOM*, pages 237–242, Baltimore, MD, USA. IEEE.

Vakilinia, I., Tosh, D. K., and Sengupta, S. (2017). Privacy-Preserving Cybersecurity Information Exchange Mechanism. In *2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, number 1, pages 1–7, Seattle, WA, USA. IEEE.

Valdes, A., Fong, M., and Skinner, K. (2006). Data cube indexing of large-scale Infosec repositories. Technical report, SRI International.

Varadarajan, G. K. (2012). Web Application Attack Analysis Using Bro IDS. Technical report, SANS Institute.

Zhang, T. and Zhu, Q. (2018). Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs. *IEEE Transactions on Signal and Information Processing over Networks*, 4(1):148–161.

Zhuang, J. and Bier, V. M. (2010). Reasons for Secrecy and Deception in Homeland-Security Resource Allocation. *Risk Analysis*.

Zhuang, J., Bier, V. M., and Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research*.