Comparing Cybersecurity Information Exchange Models and Standards for the Common Secure Information Management Framework

Jussi Simola Email: jussi.hm.simola@jyu.fi
University of Jyväskylä, Jyväskylä, Finland

Abstract

Cyber threats have increased in spite of formal economic integration in the world. Decision-makers and authorities need to respond to the growing challenge of cyberthreats by increasing cooperation. Information is one of the main facilities when the objective is to prevent hybrid threats at EU level and between the western countries. The main purpose of the study is to find out separating and combining factors concerning existing cyber information sharing models and information management frameworks in western countries. The aim is also to find out crucial factors, which affect the utilization of a common Early Warning System for the ECHO stakeholders. The main findings are that unclear allocation of responsibilities in national government departments prevents authorities from fighting together against cyber and physical threats. Responsibilities for developing cybersecurity have been shared among too many developers. Operational work concerning cyber threat prevention between European public safety authorities should be more standardized, with more centralized information management system. When the purpose is to protect the critical infrastructure of society, public safety organizations in European Union member states need proactive features and continuous risk management in their information systems. The sharing of responsibilities for standardization concerning information management systems and cyber emergency procedures between authorities and international organizations is unclear.

Keywords Information sharing, Early warning, Standards, ECHO project

1. Introduction

The purpose of this paper is to support European ECHO Early Warning Solution developers, European politicians and end users but also provide features of existing information sharing models to identify and to take into consideration territorial, organizational, managerial, legal and societal dimensions of the existing information sharing solutions, models and frameworks. The research will comprise new database for the Echo Early Warning System concept. E-EWS aims at delivering a security operations

support tool enabling the members of the ECHO network to coordinate and share information in near real-time. Echo Early Warning System will provide a mechanism for EU partners to share incident and other cybersecurity relevant data to partners within the ECHO network.

The sub-research's question focused on how it is possible to integrate US-related cyber information sharing models to Europe. Within E-ECHO consortium, there is a need to protect information sharing, information management and practices. The purpose is to propose initial risk management framework for the common early warning system. There are territorial and cultural differences between The United States of America and European Union, but technological solutions create new kind of opportunities within EU member countries to reach the same situation as USA have concerning proactive intrusion detection systems. The research needs equivalences of the concepts and other variable factors in other territory—in the area of European Union.
USA is the main actor in the field of information exchange in the western world. Therefore it is important to notice information sharing frameworks and models that are already in use in global level. There are many similarities concerning legislation and technical solutions between the unions and organizations, but also differences. It is important to separate predictive and preventive purposes, because legislation differ between the countries. Despite of the formal legislative dimension, agencies of The United States of America has enough resources to act proactively and use predictive functions in cyber space. According to they have capability already and legislative implementation for the new cybersecurity features is under the progress. This research belongs to European network of Cybersecurity centres and competence Hub for innovation and Operations project, which is part of the Horizon2020 program. The rest of this paper is divided as follows. Section 2 proposes central concepts. Section 3 handles background of the cyber information sharing. Sections 4 handles legislation and regulation. Section 5 handles relevant standards. Section 6 presents Method and Process. Section 7 handles information sharing models and frameworks. Section 8 presents findings. Section 9 presents conclusion about the research.

2. Central Concepts

CERT (Computer Emergency Response Team)
An organization that provides incident response services to victims of attacks, including preventive services (i.e. alerting or advisory services on security management). The term includes governmental organizations, academic

institutions or other private body with incident response capabilities. (European Union Agency for Cybersecurity (ENISA) [12]. The EU Computer Emergency Response Team (CERT-EU) was set up in 2012 with the aim to provide effective and efficient response to information security incidents and cyber threats for the EU institutions, agencies and bodies.

Critical Infrastructure protection (CIP) Critical Information Infrastructure Protection (CIIP)

Critical infrastructure refers to the structures and functions which are necessary for the vital functions of society. They comprise fundamental physical facilities and structures as well as electronic functions and services. Critical infrastructure (CI) includes Energy production, transmission and distribution networks, ICT systems, networks and services (including mass communication), financial services, transport and logistics, water supply, construction and maintenance of infrastructure, waste management in special circumstances. Transforming the nation's aging electric power system into an interoperable smart grid enabling two-way flows of energy and communications. That smart network will integrate information and communication technologies with the power-delivery infrastructure [428] According to Secretariat of the Security Committee [39].

Critical Information Infrastructure means any physical or virtual information system that controls, process, transmits, receives or stores electronic information in any form including data, voice or video that is vital to the functioning of critical infrastructure. Those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy [32].

Cyber-Physical Systems (CPS)

Cyber-physical systems integrate computing and communication capabilities with monitoring and control of entities into the physical world. In CPS, embedded computers and networks monitor and control the physical processes. CPS are enabling next generation “smart systems” like advanced robotics, computer-controlled processes and real-time integrated systems [25].

Cyber Threats in Critical Infrastructure

These threats can be initiated and maintained by a mixture of malware, social engineering, or highly sophisticated advanced persistent threats (APTs) that are targeted and continues for a long period of time. Channel jamming is one of the most efficient ways to launch physical-layer DoS attacks, especially for wireless communications. According to National Institute of Standards and Technology [32], National Institute of Standards and Technology [34].

ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security [6].

Information Security Management System (ISMS)

An Information Security Management System (ISMS) describes and demonstrates an organization's approach to Information Security (and privacy management). It includes how people, policies, controls and systems identify, then address the opportunities and threats revolving around valuable information and related assets.

The European Cyber Security Organisation (ECSO)

It represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public–Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

Information Exchange

According to ISO/IEC 27002 Information exchange should base on policies, procedures and agreements (e.g. non-disclosure agreements) concerning information transfer to/from third parties, including electronic information sharing (e.g., messaging).

Information Sharing and Analysis Centers (ISACs)

ISAC is collaboration community created for sector-specific national or international information sharing. Information Sharing and Analysis Centers are trusted entities to foster information sharing and good practices about physical and cyber threats and mitigation. The ISAC could support the implementation of new European legislation (e.g. NIS Directive) or support economic interests [7].

Information Sharing and Analysis Organization (ISAO)

An ISAO is any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analysing critical cyber related information in order to better understand security problems and interdependencies related to cyber systems to ensure their availability, integrity, and reliability [43].

North Atlantic Treaty Organization (NATO)

NATO is a 70 years old security alliance of 28 full member countries from North America and Europe. NATO's primary goal is to protect the Allies'

security by political and military means. NATO is the principal security instrument of the transatlantic community. The security of North America and Europe are permanently tied together with allies. NATO enlargement has furthered the U.S. goal of a Europe whole, free, and at peace [42].

Risk Assessment Framework (RAF)

According to National Institute of Standards and Technology [35], the purpose of risk assessments is to inform decision makers and support risk responses by

(a)

Identifying relevant threats to organizations or threats directed through organizations against other organizations;

(b)

Identifying internal and external vulnerabilities;

(c)

Impact to organizations that may occur given the potential for threats exploiting vulnerabilities and

(d)

Likelihood that harm will occur. The result is a determination of risk.

Risk Management Framework (RMF)

Comprehensive risk management process by NIST, which Integrate the risk Management Framework into the system development lifecycle.

Standards ISO 27000 family

This family of 27000 standards provide fundamental bases for the definition and implementation of an Information Security Management System (ISMS) [31] (JRC TAXONOMY). The Security Measurement Index is based on ISO 27000 international standards and input from an advisory board of security professionals. It consists benchmarking tools for assessing organizations' security practices, a global assessment of IT and a basis for developing security measurement best practices to help make cybersecurity more effective and efficient [22].

Among ISO 27000 family, target audience comprise e.g. personnel of risk management. Personnel as skilled lead auditors are needed to grant certification [13].

Standard ISO/IEC 27010:2015 (ISO/IEC 2700 family)

Is a key component of trusted information sharing is a "supporting entity", defined as "A trusted independent entity appointed by the information sharing community to organise and support their activities, for example, by providing a source anonymization service" [18].

Tactics, Techniques, and Procedures (TTPs)

The behaviour of an actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower level, highly detailed

description in the context of a technique (National Institute of Standards and Technology [33].

Threat Information

Any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations [33].

3.Cooperation Within the USA, NATO and EU

The Department of Homeland Security (DHS) is the U.S. Federal Government focal point of the U.S. cyber information-sharing ecosystem. It is responsible for the government's operational responses to major cybersecurity incidents, analyzing threats and exchanging critical cybersecurity information with the owners and operators of critical infrastructures and trusted worldwide partners. DHS as part of U.S Government and NATO (North Atlantic Treaty Union) have developed advanced situational awareness systems within cyber ecosystem. NATO is developing a Cyber Rapid Reaction Team (RRT) that protect its critical infrastructure. U.S. Cyber Command's Cyber Protection Teams (CPT's) creates security for all states in USA. NATO does not have an inherent cyber offensive capability, as the U.S Cyber CPT.

NATO CCD COE's mission is to enhance cooperation and information sharing between NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organizing conferences, workshops and cyber defence exercises, and offering consultations upon request [37]. NATO does not have own cyber weapons against cyber-attacks [41]. The U.S.-led alliance established an operations centre on Aug. 31.2018 at its military hub in Belgium and the U.S.A, Britain, Estonia and other allies have since offered their cyber capabilities [3]. NATO´s CYOC (CYOC Cyber Operations Center) is under development, and it will provide coordination and integration fuctions for allies.

The MITRE Corporation is a private, not-for-profit organization that manages and operates federally funded research and development centers (FFRDCs) that support United States (U.S.) government sponsors. FFRDCs serve as long-term strategic partners to the government, providing objective guidance in an environment free of conflicts of interest. MITRE has substantial experience as a trusted, independent third party providing secure stewardship, sharing, and transformational analyses of sensitive information in USA [2].

3. 1Background of Information Sharing Between U.S and EU

In 2009 ENISA (European Network and Information Security Agency) defined information exchange as follows: An information exchange is a form of strategic partnership among key public and private stakeholders. The common goal of the information exchange is mostly to address malicious cyber-attacks, natural disasters and physical attacks. The drivers for this information exchange are the benefits of member countries working together on common problems and gaining access to information, which is not available from any other sources [12].

The European Commission presented the cybersecurity strategy of the European Union in 2013. It sets out the EU approach on how to best prevent and respond to cyber disruptions and attacks as well as emphasizes that fundamental rights, democracy and the rule of law need to be protected in the cyber-atmosphere. Cyber resilience as one of the strategic priorities. That means effective cooperation between public authorities and the private sector is crucial factor [7].

The European Public-Private Partnership for Resilience (EP3R) was established in 2009 and was the very first attempt at Pan-European level to use a Public-Private Partnership (PPP) to address cross-border Security and Resilience concerns in the Telecom Sector. After the EP3R the main principles for setting up a PPP ecosystem in Europe are to provide legal basis of cooperation. It is also important to ensure open communication between public and private sector. Involvement of Small and Medium Enterprises (SMEs) in the process of PPP building is also crucial, since they are the backbone of the European economy [1114].

3.2. Information Exchange in Law Enforcement

How to prevent criminal activities has been one of the main question when public safety authorities have tried to solve a common problem within EU countries. Hague Programme and Stockholm Programme introduced the principle of availability as the guiding concept for information exchange of law enforcement. Information that is available to law enforcement authorities in one Member State should be made accessible to law enforcement authorities or public safety authorities in other Member States [27].

Regulations and Policy Documents; European Regulation and policy documents were considered as sources for legal definitions and to cover the gaps left by the vocabularies extracted from standards when dealing with non-technical definitions [27].

Law enforcement authorities can use Schengen Information Systems (SIS) to consult alerts on wanted persons etc. both inside the EU and at the EU external

border. The SIS improve information exchange on terrorist suspects and efforts Member States of EU invalidate e.g. the travel documents [27].
The European Commission has adopted a Communication on the European Information Exchange Model (EIXM). The instruments covered by EIXM allows other to exchange automatically fingerprints, DNA and vehicle registration data (Prum decision). Swedish decision sets out how information should be exchange between EU Member States [27].
Europol supports Member States of the European Union as the information hub for EU law enforcement. Its Secure Information Exchange Network Application (SIENA) enables authorities to exchange information with each other, with Europol, and with a number of third parties. Europol's databases help law enforcement from different countries to work together by identifying common investigations, as well as providing the basis for strategic and thematic analysis [27].

4. Legislation and Regulation Concerning Information Exchange in USA and Europe

4.1. Regulation in the USA

The White House designated the National Coordinating Center for Communications (NCC) as Information Sharing and Analysis Center (ISAC) for telecommunications in accordance with presidential Decision Directive 63 in 2000 (President's National Security Telecommunications Advisory Committee (NSTAC) [38].
The communications Information Sharing and Analysis Center (Comm-ISAC) incorporating dozens of organisations. It has facilitated the exchange of information among industry and government participants regarding vulnerabilities, threats, intrusions and anomalies affecting the telecommunications infrastructure.
The exchange of information between the EU and the US has been regulated among other things, as follows; The European Commission and the U.S. Government reached a political agreement on a new framework for transatlantic exchanges of personal data for commercial purposes named the EU-U.S. Privacy Shield. The European Commission adopted the EU-U.S. Privacy Shield on July of 2016 [8].
The framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers.
The EU-U.S. Privacy Shield based on the principles: Obligations on companies that handle data. (a) The U.S. Department of Commerce will

conduct regular updates and reviews of participating companies to ensure that companies follow the rules they submitted themselves to. (b) Clear safeguards and transparency obligations on U.S. government access: The US has given the EU assurance that the access of public authorities for law enforcement and national security is subject to clear oversight mechanisms. (c) Effective protection of individual rights: citizen who thinks that collected data has been misused under the Privacy Shield scheme will benefit from several accessible dispute resolution mechanisms. It is possible for a company to resolve the complaint by itself or give it to The Alternative Dispute resolution (ADR) to be resolved for free. Citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved [8]. The Court of Justice of the European Union issued a judgement declaring as invalid the European Commission´s Decision (EU) 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield Framework is no longer a valid mechanism to comply with with EU data protection requirements when sharing personal data from the European Union to the United States [45]. Participated organizations of the Privacy Shield program are required to re-certify to the Department of Commerce annually. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to achieve its annual re-certification to the Department. An organizations´s removal from the list means it may no longer claim that it benefits from the Privacy Shield.

4.1.1. Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. The FOIA requires agencies to proactively post online certain categories of information, including frequently requested records. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it comprises under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement. Any person can make a FOIA request (Office of Information Policy (OIP) [36].

4.1.2. Cybersecurity Information Sharing Act (CISA)

CISA authorizes companies to monitor and implement defensive measures on their own information systems to counter cyber threats. CISA provides certain protections to encourage companies voluntarily to share information about “cyber threat indicators” and “defensive measures” with the federal government, state and local governments, and other enterprises and private entities. These protections comprise protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some

of these protections apply only when sharing with certain entities. Qualifying these protections requires that, the information sharing must comply with CISA's requirements, including regarding the removal of personal information [16].

4.2. Regulation in the European Union

The list of the most relevant regulation taken into consideration in EU level.

4.2.1. NIS Directive

ENISA, Europol/EC3 and the EDA are three agencies active from the perspective of NIS, law enforcement and defines respectively. These agencies have Management Boards where the Member States are represented and offer platforms for coordination at EU level [10].

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 (NIS directive). The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. The NIS directive was adopted in 2016 and subsequently, because it is an EU directive, every EU member state has started to adopt national legislation, which follows or "transposes' the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example to re-use existing organizational structures or to align with existing national legislation [5]. The European Parliament resolution on the European Union's cyber Security Strategy states e.g. that the detection and reporting of cyber-security incidents are central to the promotion of information networks Sustainability in the Union [26].

The NIS Directive consist three parts:

1.

National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.

2.

Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc.

3.

National supervision of critical sectors: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc.).

4.2.2. General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy. GDPR applies to all businesses offering goods and/or services to the EU. That means that the organizations do not have to reside in the EU area or even in Europe, if you are holding private information about an EU citizen whom you provide services, GDPR applies [9]. The Regulation introduces stronger citizens' rights as new transparency requirements. It strengthens the rights of information, access and the right to be forgotten. The law is technology neutral and applies to both automated and manual processing if the data is organized in accordance with pre-defined criteria [9]. It also does not matter if the data is stored in an IT system through video surveillance, or on paper. In all these cases personal data is subject to the protection requirements set out in the GDPR.

5. Relevant Standards Concerning Cyber Secure Information Sharing

What is Data protection and relationship between 27000 and 29000 family standards?

Data protection is the basic legal right of all individuals to protect their own personal information. Personal information is any information relating to an identified or identifiable person. The purpose of data protection is to indicate when and under what conditions personal data may be processed. Organizations processing personal da ta are required to take reasonable steps to protect it [15].

How should personal data be processed?

The processing of personal data or privacy issues is subject to requirements in several different laws. The processing of personal data must be confidential and secure. The processing of personal data according to the principles is only for a specific and legitimate purpose. Privacy Policy—Consent and Freedom of Choice. Legality and definition of purpose. Limitation of data collection. Restriction of data processing. Restriction on Use, Storage and Disposal SFS-ISO / IEC 2910 [15].

Important standards of data protection

The 29000 series contains standards that fundamentally govern privacy, although the 29000 series contains a very wide variety, most of which have nothing to do with privacy issues. The 27000 series describes the standards related to the security management method, some of which also directly concern data protection. The 27000 Series management template can be used to implement a data-driven environment, which is a prerequisite for data protection [15]. As Fig. 1 illustrates, information security consist of CIA

(Confidentially, Integrity and Availability) features. Confidentiality means that information is only accessible to those entitled to it.

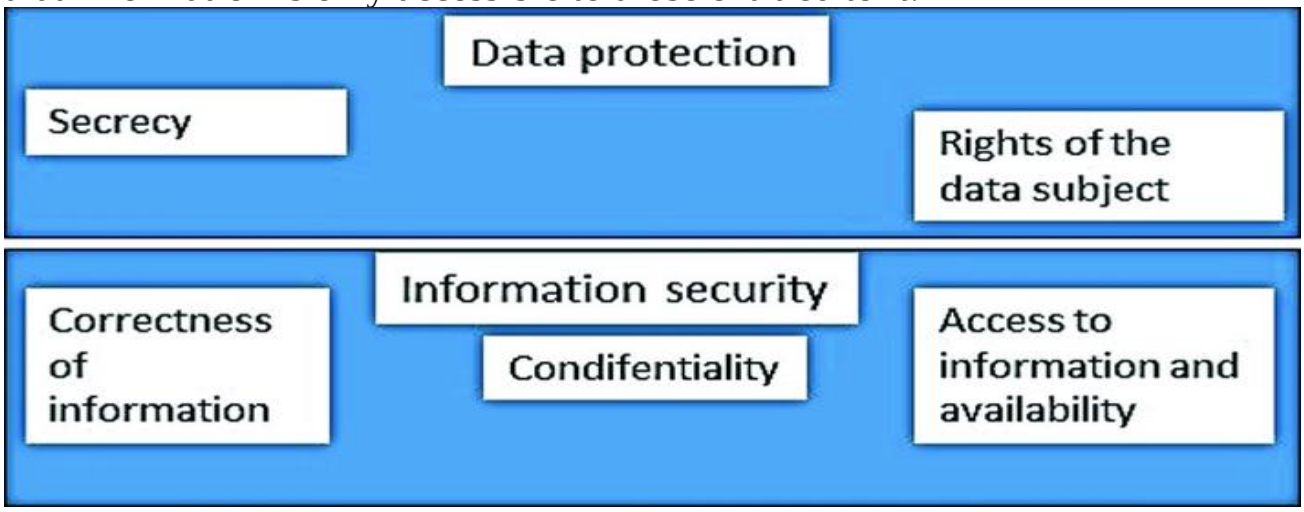

Fig. 1 Privacy elements (CIA)

Integrity or correctness of information means that the information must be true and correct. Availability means that information is available when you want to use the data of the data subject. The right to privacy or the rights of the data subject required by data protection cannot be fulfilled without the implementation of the data security attributes as mentioned above. For example, the data subject has the right to know who has accessed the data stored in the register. This requires confidentiality and integrity. Figure 2 presents relationships between the elements of data protection and relationships between the elements of data protection and standards (modified from SFS 2018 publication).

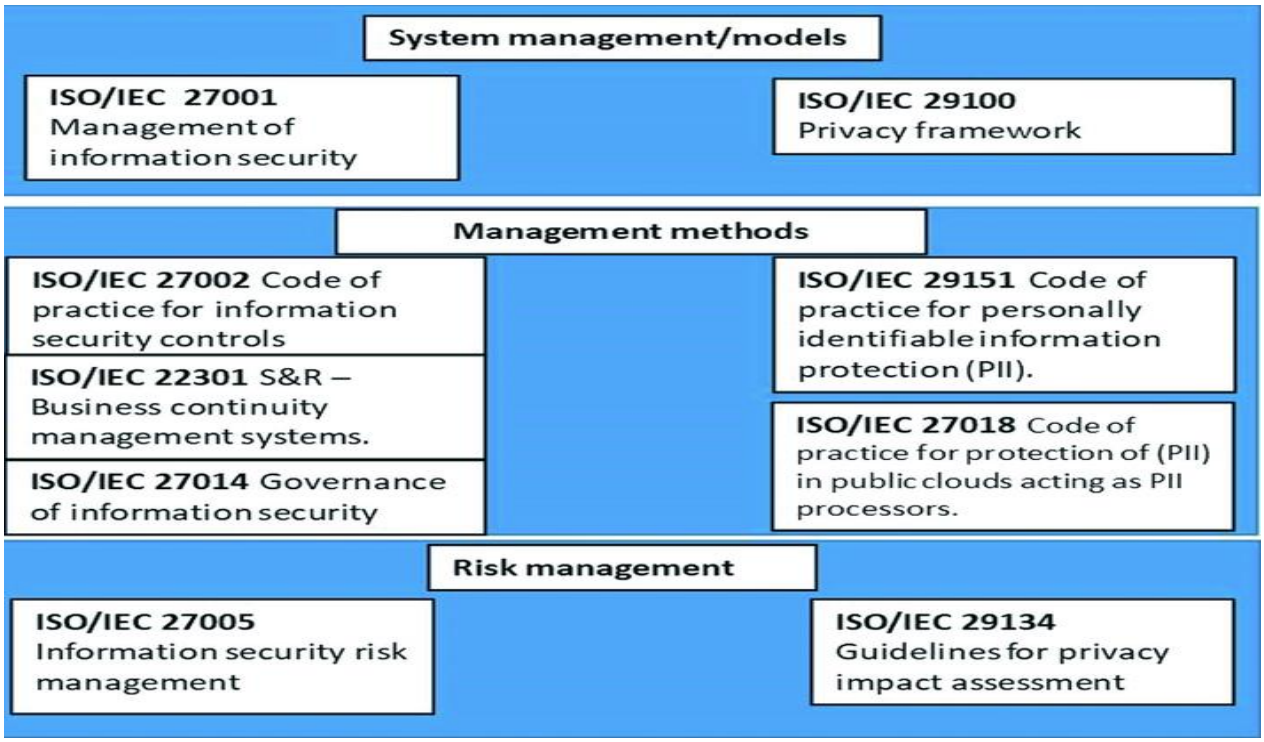

Fig. 2 Elements of the data protection

According to ISECT [23] risk management, ISO/IEC 27005 is a remarkable standard which propose ongoing process consisting of a structured sequence of activities, some of which are iterative:
Establish the risk management context (e.g. the scope, approaches or methods to be used and relevant policies and criteria such as the organization's risk tolerance)
Quantitatively or qualitatively assess means identify, analyze and evaluate relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a "level of risk".
Manage and modify by using information security controls, retain or "accept", avoid and/or share with third parties the risks appropriately, using those "levels of risk" to prioritize them;
Keep partners informed throughout the process; and Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes [23].
ISO/IEC 29134:2017 [19] gives guidelines for a process on privacy impact assessments and a structure and content of a PIA report. It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations. ISO/IEC 29134:2017 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII [19].
According to requirements for system management ISO/IEC 29100:2011 provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology. It is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII [17].
ISO/IEC 27001 formally specifies an Information Security Management System (ISMS). It is a suite of activities concerning the management of information risks (called "information security risks" in the standard). The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information risks. The

ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts—an important aspect in such a dynamic field, and a key advantage of ISO27 family's flexible risk-driven approach. "Statement of Applicability" (SoA) is not explicitly defined, it is a mandatory requirement. SoA refers to the output from the information risk assessments and in particular the decisions around treating those risks. The SoA may, i.e. take the form of a matrix identifying various types of information risks on one axis and risk treatment options on the other and show how the risks are to be treated in the body, and perhaps who is accountable for them. It usually references the relevant controls from ISO/IEC 27002 but the organization may use a completely different framework such as NIST SP800-53, the ISF standard, BMIS and other [24].

Management methods and controls

Management consists ISO/IEC 29151:2017 and ISO/IEC 27002:2013. ISO/IEC 29151:2017 establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). ISO/IEC 29151:2017 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII [21].

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). It is designed to be used by organizations that intend to: select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001; implement commonly accepted information security controls; develop their own information security management guidelines [20].

Continuity management and relationship to the Cyber-Physical System

ISO/IEC 22301:2019 set frames to the Security and resilience. It consists requirements for business continuity management systems. It represents how to manage business continuity in an organization [1]. This standard based on leading business continuity specialists opinions and supplies the framework for managing business continuity in an organization [1]. Other relevant standards are listed on the figure 3.

6. Method and Process of the Research

Case study illustrates the attempt to produce a profound and detailed information about the object under research. The materials collected for this case study based on scientific publications, official documents, collected

articles and literary material. The research is focused on how it's possible integrate USA- related information sharing models in European level. Yin [44] identifies five components of research design for case studies: (1) the questions of the study, (2) its propositions, if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. This case study is carried out with the guidance of Yin [44].

There are country-specific differences, institutional differences, legislative differences in legislation, etc. The purpose is to categorize things into their own groups. Some information sharing models and information management frameworks are simple diagrams, some are ready-made templates, and some information sharing models have concrete instruments and tools. The purpose of the analysis is to find out about the functionalities, useful standards and features of information sharing systems in the EU, USA and NATO. Outcome of the research is combined proposal of information sharing model and initial risk management framework.

7. Definition of Information Sharing Goals

According to National Institute of Standards and Technology [33] the organization should establish goals and objectives that describe the desired outcomes of threat information. These objectives will help guide the organization through the process of scoping its information sharing efforts, joining sharing communities and providing ongoing support for information sharing activities.

According to Skopik et al. [40] primary dimensions of security information sharing can be divided as follows: (a) Cooperation and coordination economic need for coordinated cyber defense. There exists variety of classification of information that are viable for a wide range of stakeholders: indicators of compromise, technical vulnerabilities, zero-day exploits, social engineering attacks or critical service outages. (b) Legal and Regulatory Atmosphere: information sharing requires a legal basis. Therefore, the European Union and its Member States and the US, have already done a set of directives and regulations. (c) Standardization Efforts means enabling information sharing, standards and specifications need to standardize that are compliant with legal requirements (e.g. NIST, ENISA, ETSI and ISO). (d) Regional and International Implementations means taking these standards and specifications, organizational measures and sharing structures need to be realized, integrated and implemented. CERTs and national cyber security centers work on this issue. (e) Technology Integration into Organizations means sharing protocols and management tools on the technical layer need to be selected and set into operation.

7.1. Identify Internal Sources of Cyber Threat Information

CORA (Cyber Operations Rapid Assessment) methodology was developed to study issues and best practices in cyber information sharing. In addition, it consists as an engagement tool for assessing and improving threat-based security defenses. CORA identifies five major areas of cyber security where the proper introduction of threat information can have tremendous impact on the efficacy of defenses: External Engagement—Tools and Data Collection—Tracking and Analysis—Internal Processes—Threat Awareness and Training.

The TICSO gather cyber threat intelligence and information from a variety of sources including open source reporting by researchers and consultants, government and law enforcement sources [USCERT, INFRG], fee-for-service threat Intel feeds from vendors and industry sector and regional threat sharing communities such as ISACs and ISAOs. The TICSO focuses collection efforts on the most relevant information by defining prioritized intelligence requirements (PIR), and continuously evaluating the quality of intelligence from different sources in terms of relevance, timeliness, and accuracy (MITRE Corporation).

A first step in any information sharing effort is to identify sources of threat information within an organization. According to National Institute of Standards and Technology [33]. The process of identifying threat information sources includes the following sections:

(a)

Identify sensors, tools, data feeds, and repositories that produce threat information and confirm that the information is produced at a frequency, precision, and accuracy to support cybersecurity decision-making.

(b)

Identify threat information that is collected and analyzed as part of an organization’s continuous monitoring strategy.

(c)

Locate threat information that is collected and stored, but not necessarily analyzed or reviewed on an ongoing basis.

(d)

Identify threat information that is suitable for sharing with outside parties and that could help them more effectively respond to threats. Examples of selected Internal Information Sources [33].

7.2. Comparing Features of the Information Sharing Models

There are several different information sharing models in the world. The most important thing was to choose such cyber information sharing models that are widely used in the European Union countries, USA and NATO. It is not necessary to compare all models or frameworks because availability of

information varies a lot. Usually the information-sharing model is incomplete frame that is believed to solve all the problems concerning cyber security. As Table 1 illustrates five different type of models has chosen to more detailed review.

Table 1

Examples of information sharing models

Organization //Name //System/model or framework type	**Main tasks/ features**	**Special tasks or info**	**Major areas of cyber impacts**	**Instruments**
MITRE// CORA // Assessment of cyber operations (not-for-profit organization)	Developed for to study issues and best practices in cyber information sharing. It serves as an engagement tool for assessing and improving threat-based security defences	Based on NIST Special Publication 800–150: Guide to Cyber Threat Information Sharing	External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	indicators scan networks and systems— Reporting new indicators about attacks on its own networks
MITRE// TISCO// Threat-Informed Model	It collects cyber threat intelligence and information from a variety of sources including open source reporting by researchers and consultants		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Sensors monitoring attack activity such as phishing email addresses and URLs of malicious sites, host-based indicators
ENISA// ISAC// Member driven organization model Country-focused ISAC - International ISAC -	Sharing knowledge about incidents with the member organizations and prevent/ respond to the incidents which occur (ISAC is a fast way to get all the knowledge and way of networking	ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It provides information about threats and incidents. (close cooperation with the industry, public	(a) Some information can be shared widely with all members. (b) The shared information is more detailed in internal circle. c) use of the (TLP) to share	web portal/platform (following a specific template) and encrypted emails

Table 1

Examples of information sharing models

Organization //Name //System/model or framework type	**Main tasks/ features**	**Special tasks or info**	**Major areas of cyber impacts**	**Instruments**
	and meeting people from different organizations	entities get better understanding of the private sector)	information	
ENISA// PPP// Cooperative model	Access to public funds. Opportunity to influence national legislation and obligatory standards. Access to public sector knowledge and confidential information (EU legislation, fighting against cybercrime)	Helps to achieve resilience in the cyber ecosystem. PPP Increase the trust between public-public–private. it allows to have better information and proactive attitude in case of crisis	Incident handling and crisis management, Information exchange, Early warnings, Technical evaluation, Defining standards etc.	Help desk helps PPP's members. PPP does not consist real-time instruments against cyberattacks
NIST// Framework//	NIST FW targeting on risk management, procedures and privacy preservation aspects	The guidelines included in the ISO/IEC27010 standard, it is oriented toward the protection of the data exchanged in the information sharing process	Techniques standards and protocols for systems monitoring, threat detection, vulnerability inventory and incident exchange	Framework adds consist different kind of tools, but only framework does not offer protection for shared information or information for incident handling process

8. Findings

Mechanism type of the ISAC concerns the overall structure that is used to exchange information. This type of mechanism often has a central hub that receives data from the participants. The hub can redistribute the incoming data directly to other members, or it can provide value-added services and send the

updated information or data to the members. The hub may act as a “separator” that can facilitate information sharing while protecting the identities of the members. One of the main tasks of ISACs is sharing information on intrusions and vulnerabilities. These types of information are usually troublesome; therefore, companies often decide to keep silent. ISAC hub system relies on the functionality of the hub, which makes the system vulnerable to delays and systemic failures [29]. Important information is often unnecessary to achieve, delays in information sharing can reduce the benefits of the information-sharing hub mechanism. In post to all model information is shared among stakeholders. MITREs model is one kind of hybrid information sharing model. It is a partner for helping private or public organizations stand-up and run information sharing exchanges. Mechanism of MITRE use automated processing of information. This work has enabled security automation in vulnerability management, asset management, and configuration management though the Security Content Automation Protocol program. Members of MITRE do not share information. Each participant sends its sensitive data to MITRE, and MITRE works diligently to ensure that member data is kept confidential [29].

There is a need to develop Public–Private information-sharing models in EU level because public safety organizations of the Department of the Homeland Security in USA are capable to handle external threats more effectively. There are international organizations which have formulated co-operational working environment such a way that western world could operate for the common purpose. International organizations like UN (United Nations) and NATO are the connecting factors concerning harmonization of information sharing procedures in the EU and USA and between them, not forgetting NATO. In this author’s view, the so-called “triangle” should be called a “square.”

The requirements of the system integrity means that it’s impossible to separate information system -related standards from the information sharing methods when the purpose is to design common cyber ecosystem for the western world. Interoperability should be coordinated through standards as Fig. 3 illustrated.

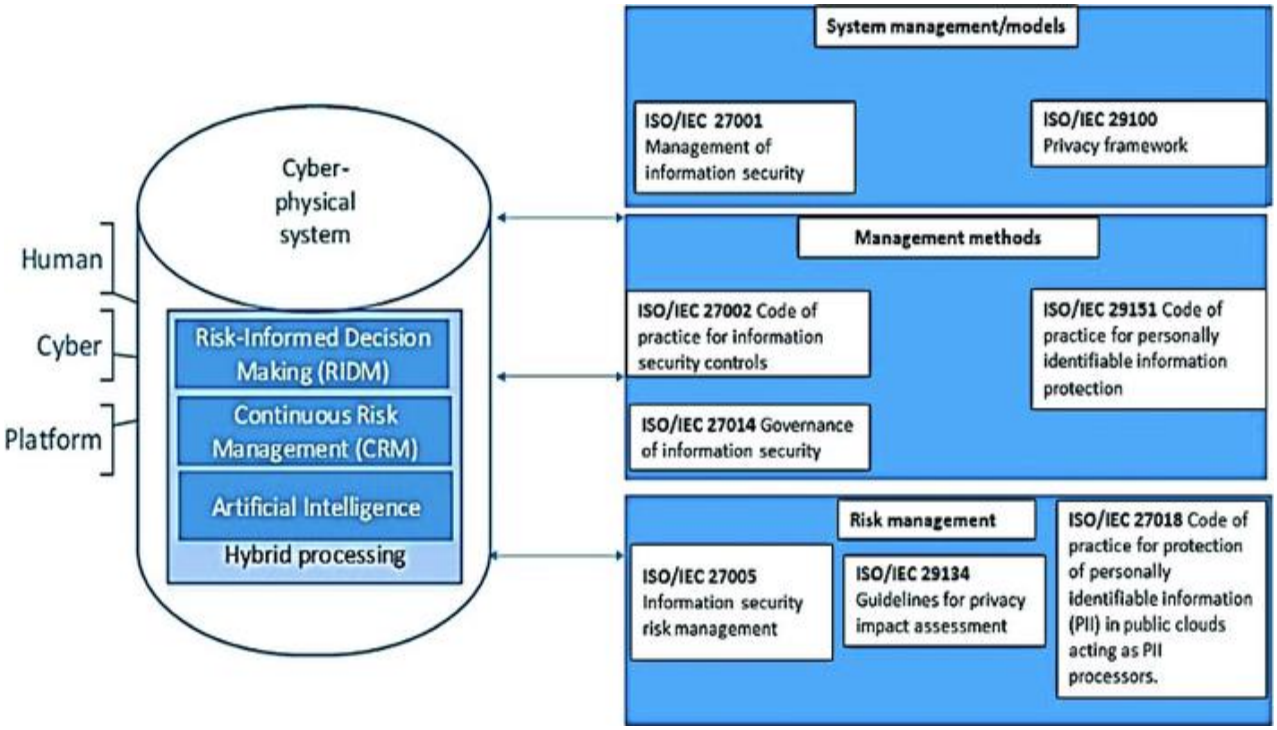

Fig. 3 Relationship between CPS and continuous risk management system

Cyber-physical system allows to protect critical infrastructure because of the automated functionalities. E.g., in a finance sector it is not possible to protect it without interfering with the activities of the attacker. Automated physical actions mean Physical functionalities e.g., in finance sector and/or cyber-defence functionalities against the attacks but everything must be reverted to existing standards. Privacy impact (PI) is crucial element in all situations when the purpose is to develop system which handle privacy identifiable information. PI could result from the processing of Privacy Identifiable information (PII). According to ISO/IEC 29134:2017 (International Organization for Standardization (ISO) [19] a Privacy Impact Assessment (PIA) is a tool for addressing the potential impacts on privacy of a process information system, programme, or device. It will inform to all participants which have to take actions in order to treat privacy risk. PIA is ongoing process and report may include documentation about measures taken for risk treatment, measures may arise from the use of the ISMS.

At a general level, collaboration between cyber-physical system and continuous risk management requires collaboration between these elements. In the traditional sense, three levels can be found; human; platform layer and cyber layer as figure illustrates, but that’s not enough. Proposed framework require to take into account standards and information management when purpose is to develop common early warning solution for the western allies.

At the technical level, the challenge of semantic interoperability is that information systems should automatically understand the concepts arising

from the actions of people and organisations. Therefore, it is important to create a common risk management framework for both. It is possible to connect different kind of decision-making strategies to the cyber physical framework as proposal illustrates above. Legislation and regulation must be the fundamental basis for all functions and operations.
This means that fundamental frame of the cyber-physical system based on legislation, rules and standards. E.g., higher-level EWS should be structured from the view of "regulation". The operations of the system must be based on rules and standards. Semantic interoperability means that an information system is able to combine the information it receives from different sources and process it in a way that preserves the meaning of the information. E.g., there are business-related differences concerning sector-specific stakeholders of the ECHO consortium.

9. Conclusions

Separate functionalities between the EU member states are not only problem. When the common goal is to improve Cyber Situational Awareness, it is important to deepen the cooperation between western stakeholders. Major problem of information sharing models is related lack of real-time cyber information management between participants. There is essential problem with features of information sharing models. When the purpose is to protect vital functions of society, public safety organizations in European Union member states needs proactive features in their information systems. A shared common cyber situational awareness means that real time communication links between the states must exist.
Legislation is not only factor, which affects to completely secure cyber-ecosystem. Developed systems need coherent standardization, common management system and governance model. The USA and its public safety cyber defense organizations has ability to combat cyberattacks, which have made against vital functions, but also make counter-attacks [41]. It is one of the most important features in protecting the western world. Cooperation and collaboration in triangle EU-NATO-USA is therefore particularly important. In addition The United Nations acts as the fourth element. Utilizing the best features of the information sharing models will ensure procedures of continuity management. It is therefore important to place EU countries in the right context. Legislation has been harmonized, but occasional is to trust organization's functionalities. Common continuous risk management system helps to handle the databases concerning privacy issues. Lack of standardization may cause obstacles when the aim is to catch cyber criminals or find out state level actor that has caused a cyber or hybrid attacks.

It is a fundamental problem that, as the geographical area of the European Union expands, it does not have the capability to prevent hybrid-threats. Controlled governance model for the EWS and common standardization concerning information management systems and cyber emergency procedures between authorities, and international organizations helps to achieve common situational awareness inside the western world. It is not enough that every country tries to tackle cyberthreats separately. There is a need for a jointly controlled information exhange framework for the EU countries and credible counter opeartion tools for counter-attack operations that must be connectable to another defense mechanism. Nato is setting up a joint coordination center against cyberattacks by 2023, but NATO will also neeed centralized mechanism to defend allies against cyber-threats.

References

1. Advisera Expert Solutions: What is ISO 22301? [Homepage of Advisera Expert Solutions] (2019). [Online]. Available: https://advisera.com/27001academy/what-is-iso-22301/. 28 Aug 10

2.´ Bakis, B., Wang, E.D.: Building a National Cyber Information-Sharing Ecosystem. MITRE Corporation (2017)

3. Bigelow, B.: The Topography of cyberspace and its consequences for operations. In: 10th International Conference on Cyber Conflict 2018, NATO CCD COE Publications (2018)

4. Department of Homeland Security (DHS): Blueprint for a Secure Cyber Future—The Cybersecurity Strategy for the Homeland Security Enterprise. DHS (2011)

5. NISA: NIS Directive [Homepage of European Union Agency for Network and Information Security] (2019-last update), [Online]. Available: https://www.enisa.europa.eu/topics/nis-directive [6/2019]

6. ENISA: Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS). European Union Agency for Network and Information Security, Greece (2013)

7. ENISA & ITE: Information Sharing and Analysis Centres (ISACs) Cooperative models. European Union Agency for Network and Information Security, Greece (2017)

8. European Commission: EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows. Brussels (2016a)

9. European Commission: General Data Protection Regulation (EU) 2016/679. Regulation edn. Brussels (2016b)

10. European Commission: Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions. European Commission, Brussels (2013)

11. European Union Agency for Cybersecurity (ENISA): Public Private Partnerships (PPP) Cooperative models. European Union Agency for Network and Information Security, Greece (2017)

12. European Union Agency for Cybersecurity (ENISA): Good Practice Guide—Network Security Information exchanges. ENISA, Greece (2009)

13. European Union Agency for Network and Information Security (ENISA): Smart grid security certification in EUROPE. ENISA, Greece (2014)

14. European Union Agency for Network and Information Security (ENISA): EP3R 2013—Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS). European Union Agency for Network and Information Security, Greece (2013)

15. Finnish Association for Standardization SFS RY: Information technology. Safety. Information security management systems. Privacy Standards. SFS (2018)

16. Harvard Law School Forum on Corporate Governance and Financial Regulation: Federal Guidance on the Cybersecurity Information Sharing Act of 2015 [Homepage of The President and Fellows of Harvard College] (2016). [Online]. Available: https://corpgov.law.harvard.edu/2016/03/03/federal-

guidance-on-the-cybersecurity-information-sharing-act-of-2015/. 11 Oct 2019

17. International Organization for Standardization (ISO): ISO/IEC 29151:2017 Information technology—Security techniques—Code of practice for personally identifiable information protection [Homepage of ISO] (2018), [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:29151:ed-1:v1:en

18. International Organization for Standardization (ISO): International Standard ISO/IEC 27010:2015. Standard edn. Switzerland (2015)

19. International Organization for Standardization (ISO): ISO/IEC 29134:2017 Guidelines for privacy impact assessment (2017). Available: https://www.iso.org/standard/62289.html

20. International Organization for Standardization (ISO): ISO/IEC 27002:2013 Security techniques—Code of practice for information security controls [Homepage of ISO] (2013), [Online]. Available: https://www.iso.org/standard/54533.html

21. International Organization for Standardization ISO: ISO/IEC 29100:2011 information technology—Security techniques—Privacy framework [Homepage of ISO] (2018), [Online]. Available: https://www.iso.org/standard/45123.html2019

22. International Telecommunication Union: Global Cybersecurity Index (GCI) 2018. ITU, Switzerland (2018)

23. ISECT: ISO/IEC 27005:2018 Information technology—Security techniques—Information security risk management (third edition [Homepage of IsecT Limited] (2018), [Online]. Available: https://www.iso27001security.com/html/27005.html

24. ISECT: ISO/IEC 27001 Information security management systems—Requirements [Homepage of IsecT Limited] (2017), [Online]. Available: https://www.iso27001security.com/html/about_us.html

25. Lee, E.A., Seshia, S.A.: Introduction to Embedded Systems, A Cyber-Physical Systems Approach, 2 edn. (2015)

26. Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., Salminen, M.: Kyberturvallisuuden strateginen johtaminen Suomessa. 28. Valtioneuvoston kanslia, Helsinki (2018)

27. Migration and Home Affairs: Information exchange [Homepage of European Commission] (2019), [Online]. Available: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en [06/2019, 17/06/2019].

28. Ministry of the Interior: National Risk Assessment. Ministry of the Interior, Helsinki (2018)

29. MITRE: Cyber Information-Sharing Models: An Overview. MITRE Corporation (2012)

30. MITRE Corporation: Cyber Operations Rapid Assessment (CORA): A Guide to Best Practices for Threat-Informed Cyber Security Operations | The MITRE Corporation. Available: https://www.mitre.org/sites/default/files/publications/pr_15-2971-cyber-operations-rapid-assessment-best-practices_0.pdf [3/20/2016, 2016]

31. Nai-Fovino, I., Neisse, R., Lazari, A., Ruzzante, G., Polemi, N., Figwer, M.: European Cybersecurity Centres of Expertise Map—Definitions and Taxonomy. Publications Office of the European Union, Luxemburg (2018)

32. National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity. 1.1. NIST (2018)

33. National Institute of Standards and Technology: Guide to Cyber Threat Information Sharing. NIST Special Publication 800–150. National Institute of Standards and Technology, Gaithersburg (2016)

34. National Institute of Standards and Technology: Guidelines for Smart Grid Cybersecurity—Volume 2 privacy and the Smart Grid. U. S. Department of Commerce (2014)

35. National Institute of Standards and Technology: Guide for Conducting Risk Assessments. 800–30. U.S. Department of Commerce, Gaithersburg (2013)

36. Office of Information Policy (OIP): What is FOIA? [Homepage of U.S. Department of Justice] (2019), [Online]. Available: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [10/11, 2019].

37. Pernik, P., Wojtkowiak, J., Verschoor-Kirss, A.: National Cyber Security Organisation: United States. CCDCOE, Tallinn (2016)

38. President's National Security Telecommunications Advisory Committee (NSTAC): Report to the President on the National Coordinating Center. Department of the Homeland Security (2006)

39. Secretariat of the Security Committee: Finland's cyber security strategy—government resolution. Ministry of Defense (2013)

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

41. Smeets, M.: NATO Allies Need to Come to Terms with Offensive Cyber Operations [Homepage of Lawfare] (2019), [Online]. Available: https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations [11/19, 2019].

42. U.S. Mission to NATO: About NATO (2019). Available: https://nato.usmission.gov/our-relationship/about-nato/

43. White, G., Lipsey, R.: ISAO SO Product Outline. ISAO Standards Organization (2016)

44. Yin, R.K.: Case Study Research, Design and Methods, 5th edn. Sage, Thousand Oaks, CA (2014)

45. Court of Justice of the European Union: The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield (2020)