Information & Security

J. Simola, vol. 43, no. 2 (2019): 175-195
https://doi.org/10.11610/isij.4315

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Comparative Research of Cybersecurity Information Sharing Models

Jussi Simola

Laurea University of Applied Sciences R&D, Espoo Finland, https://www.laurea.fi/en/

ABSTRACT:

Cyber threats are on the increase. Authorities need to respond to growing challenges by increasing cooperation. Information sharing or information exchange in the EU level and between the countries is a main facility when the objective is to prevent hybrid threats. Intensifying relationships with private sector companies has become very important function and operating model to authorities to provide cyber-safe atmosphere. The main purpose of this study is to find out separating and combining factors concerning cyber information sharing models. The aim is also to find out nation level factors, which affect the utilization of a common Early Warning system by the ECHO stakeholders.

Summary of findings: unclear allocation of responsibilities in national government departments prevents authorities from fighting together against cyber and physical threats. Cybersecurity responsibilities have been spread too widely. Operational work concerning cyber threat prevention between European public safety authorities should be more standardized, with more centralized management. When the purpose is to protect vital functions of society, public safety organizations in EU member states need proactive features in their information systems. An essential factor in information exchange is the place of registration of organizations or companies. Unclear standardization concerning cyber emergency procedures between authorities and organizations and lack of co-operation between cyber situation centres and cyber emergency response centres prevent common situational awareness.

ARTICLE INFO:

RECEIVED: 20 JUN 2019
REVISED: 03 SEP 2019
ONLINE: 21 SEP 2019

KEYWORDS:

information sharing, Early Warnings, situational awareness, cooperation, ECHO project, indicators

E-mail: juhemisi@student.jyu.fi

Introduction

The purpose of this paper is to assist ECHO and E-EWS developers, European decision-makers 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. With the E-EWS ECHO stakeholders can retain their fully independent management of cyber-sensitive information and related data management. 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 transfer US- and NATO-related cyber information sharing models to Europe. The United States of America and European Union has a lot of similarities, but many differences. It is important to notice how global markets divide and integrate our entities where we live. There are territorial and cultural differences between the countries, but technological solutions create new kind of opportunities within EU member countries to reach the same situation as USA have concerning quality and quantity of threat-informed data. Comparative 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 sharing in the western world. Therefor 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. Agencies of The United States of America have enough resources to act proactively and use predictive functions in cyber space. This research belongs to European network of Cybersecurity centres and competence Hub for innovation and Operations, which is part of 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 Method and Process. Section 5 presents information sharing models and frameworks. Section 6 presents findings. Section 7 presents conclusion about the research.

Alert and Detection System

An alert and detection system produces information, which makes it possible to alert other players about a detected threat and develop better means of detection. Clients can determine what sort of data the system processes and the ownership of the data remains with the company itself, in its own devices. The information on situation awareness provided by the system increases understanding about the organization’s own and general state of information security.

CSIRT (Computer Security Incident Response Team) or 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.[1] 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) and Critical Information Infrastructure Protection (CIIP)

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.[2, 3] According to the Secretariat of the Security Committee of Finland, Critical infrastructure refers to the structures and functions which are necessary for the vital functions of society.[4] They comprise fundamental physical facilities and structures as well as electronic functions and services.

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.[5]

Cyber Threats in Critical Infrastructure

Cyber threats include denial of service (DoS), unauthorized vulnerability probes, botnet command and control, data exfiltration, data destruction or even physical destruction via alternation of critical software/data. 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 the US National Institute of Standards and Technology,[6, 7] Cyber-Physical attacks can be classified into three broad sections:

Physical attacks informed by cyber

The use of information gathered by cyber means that allows an attacker to plan and execute an improved or enhanced physical attack. For example, if an enemy has decided to destroy components within a substation though they are not sure which substation or components would have the greatest impact. They could access confidential information or aggregate unprotected information by cyber and they could then physically attack that specific substation and lines.

Cyber-attacks enhancing physical attacks

An enemy uses cyber means to improve the impacts of a physical attack by either making the attack more successful (e.g., greater consequences) or interfering with restoration efforts (thereby increasing the duration of the attack). Inadvertent actions could also cause such an attack. One example is an enemy tampering with the integrity of protective relay settings prior to a physical attack on power lines. Although the original settings were designed to contain the effects of a failure, the tampered settings allow the failure to cascade into impacts on a wider segment of the grid.

Use of a cyber-system to cause physical harm

An adversary uses a cyber-system that controls physical equipment in such a manner to cause physical harm/damage. An example of this is the burner management system for a natural gas generator. In this case, an adversary or a careless operator could attempt to turn on the natural gas inflow without an ignition source present. As the burner unit fills with natural gas, the adversary could turn on the ignition source, potentially causing an explosion.

Good cyber, physical and operational security planning and implementations can minimize these impacts of cyber physical attacks. Defensive measures that can be used to minimize the likelihood of successful cyber-attacks and physical attacks will also work to minimize the impacts of a cyber-physical attack.

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. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA provides recommendations on cybersecurity, supports policy development and its implementation, and collaborates with operational teams throughout Europe.[8]

National Regulatory Authority (NRA)

NRAs can play different roles in relation to cybersecurity. In Finland, for example, the tasks are: Steering and supervision of telecoms operators' operations, information security and preparedness, for example, monitoring compliance with the

information security regulation, steering and supervision of strong electronic identification and the provision of qualified certificates, for example, monitoring compliance and carrying out annual audits of certification authorities providing qualified certificates.[9]

The European Cyber Security Organization (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 Sharing and Analysis Centres (ISACs)

ISAC is collaboration community created for sector-specific national or international information sharing. Information Sharing and Analysis Centres 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,[10] or support economic interests.[11]

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.[12]

Industrial Internet of Things (IIOT)

IIOT collects data from connected devices (i.e., smart connected devices and machines) in the field or plant and then processes this data using sophisticated software and networking tools. The entire IIOT requires a collection of hardware, software, communications and networking technologies. The major area where IOT deals with energy management systems is the smart grid. IOT extends the benefits of smart grid beyond the automation, distribution and monitoring being done by the utilities.[13]

Risk Assessment Framework (RAF)

According to the National Institute of Standards and Technology,[14] the purpose of risk assessments is to inform decision makers and support risk responses by:

- Identifying relevant threats to organizations or threats directed through organizations against other organizations;
- Identifying vulnerabilities both internal and external to organizations;
- Impact to organizations that may occur given the potential for threats exploiting vulnerabilities and

- 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.

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."[15]

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.[16]

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.[17]

Organizational Bases of Cybersecurity 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, analysing 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 (CPTs) creates security for all states in USA. NATO does not have an inherent cyber offensive capability, as the U.S Cyber CPT has.

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.[18] NATO does not have own cyber weapons against

cyber-attacks. The U.S.-led alliance established an operations centre on August 31, 2018 at its military hub in Belgium and the USA, Britain, Estonia and other allies have since offered their cyber capabilities.[19]

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.[20]

Background of Information Exchange among USA and EU

Are there differences between information sharing, transferring information and information exchange? In 2009 ENISA, the European Network and Information Security Agency, defined the difference 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.[21]

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 – the national Network and Information Sharing competent authorities should collaborate and exchange relevant information with other regulatory bodies.[22]

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.[23, 24]

Development of Information Exchange in Law Enforcement

How to prevent criminal activities has been one of the main questions 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.[25]

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.[26]

The Schengen Information Systems (SIS) is widely used information sharing tool today. Law enforcement authorities can use it 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). The Swedish decision sets out how information should be exchange between EU Member States.[28]

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.[29]

Legislation and regulation concerning information exchange in USA and Europe

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.

The communications Information Sharing and Analysis Center (Comm-ISAC) incorporating dozens of organizations. 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.[30]

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. The Ombudsperson mechanism means that an independent senior official within the U.S. Department of state will ensure that complaints are properly investigated and addressed in a timely manner.[31]

Regulation in European Union

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

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.

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, or the *NIS Directive* 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.[32] 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.[33]

The NIS Directive consist of 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).

General Data Protection Regulation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, or the General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and was designed to 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.[34] The Regulation introduces stronger citizens' rights as new transparency requirements. It strengthens the rights of information, access and the right to be forgotten. The GDPR protects personal data regardless of the technology used for processing that data. The law is technology neutral and applies to both automated and manual processing if the data is organized in accordance with pre-defined criteria.[35] 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. Personal data consists of, for example; name, address, email address, an internet protocol address, location data on a mobile phone and a cookie ID, and the advertising identifier of your phone.

Other Relevant Regulations

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).
- European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cybersecurity (2011/2284(INI)) (CIIP)
- COM(2017) 477 final 2017/0225 (COD) Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency," and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
- COM(2016) 705 final Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Space Strategy for Europe"
- JOIN(2014) 9 final - Joint Communication to the European Parliament and the Council "For an open and secure global maritime domain: elements for a European Union maritime security strategy"

- JOIN(2016) 18 final Joint Communication to the European Parliament and the Council "Joint Framework on countering hybrid threats a European Union response"
- EU Cyber Defence Policy Framework [Concilium 15585/14] and Joint Communication on "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," February 2013 [JOIN(2013)1].[36]

Method and Process

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, collected articles and literary material. The research is focused on how it is possible iterate USA-related research concerning cyber information sharing models in Europe. Yin identifies five components of research design for case studies:[37] (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 following the guidance by Yin.

There are country-specific differences, institutional differences, etc. legislative differences in legislation, etc. The purpose is to categorize things into their own groups. Some models 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 and features of information sharing systems in the EU, USA and NATO. The results of the research will be utilized in developing the echo early warning system.

Definition of information sharing

According to NIST,[38] 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.

Define information sharing goals

According to Skopik and co-authors,[39] the primary dimensions of security information sharing can be divided as follows: a) Cooperation and coordination economic need for coordinated cyber defence. 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 centres 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.

Identify Internal Sources of Cyber Threat Information

The 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 defences. CORA identifies five major areas of cyber security where the proper introduction of threat information can have tremendous impact on the efficacy of defences: 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.[40] Examples of PIRs include:

- Threats and threat actors that have attacked your specific organization previously
- Vulnerabilities and exploits that pertain to technology specific to your organization or industry
- Threats and attacks against industry/sector peers or business partners.[41]

A first step in any information sharing effort is to identify sources of threat information within an organization. By conducting an inventory of internal threat information sources, an organization is better able to identify knowledge gaps. The process of identifying threat information sources includes the following sections: [42]

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 analysed as part of an organization's continuous monitoring strategy;

c) Locate threat information that is collected and stored, but not necessarily analysed 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.

Table 1 provides illustration through modified examples of selected internal cybersecurity-related information sources with human factors from NIST.

Table 1. Examples of cyber threat sources (modified from NIST).[43]

Human Factors & Network Data Sources		Human Factors & Host data Sources	
Sources	*Examples*	*Sources*	*Examples*
Router, firewall, equipment, Wi-Fi, remote services (such as remote login or remote command execution), and Dynamic Host Configuration Protocol (DHCP) server logs	Timestamp Source and destination IP address Domain name TCP/UDP port number Media Access Control (MAC) address Hostname Action (deny/allow) Status code Other protocol information	Operating system and application configuration settings states and logs	Bound and established network connection and port Process and thread Registry setting, Configuration file entry, Software version and patch level information Hardware information, User and group File attribute (e.g., name, hash value, permissions, timestamp, size) File access System event (e.g., startup, shutdown, failures), Command history
Diagnostic and monitoring tools (network intrusion detection and prevention system), packet capture & protocol analysis	IP address, port, and other protocol information Network flow data Packet payload Application-specific information Type of attack (e.g., SQL injection, buffer overflow) Targeted vulnerability Attack status (success/fail/blocked)	Antivirus products	Hostname, IP and MAC address, Malware name and type (e.g., virus, hacking tool, spyware, remote access) File name and location (i.e., path) File hash Action taken (e.g., quarantine, clean, rename, delete)
Human Factors & Other Data Sources		Web browsers	Browser history and cache including: Site visited; Forms, Social media platforms, Object downloaded; Object uploaded; Browser extension installed or enabled; Cookies; Transactions
Security Information and Event Management (SIEM)	Summary reports synthesized from a variety of data sources (e.g., operating system, application, and network logs)		
Email systems	Email messages: Email header content - Sender/recipient email address - Subject line - Routing information Attachments, URLs, Embedded graphic		
Help desk ticketing systems, incident management/tracking system and human activity within the organization	Analysis reports and observations regarding: TTPs, campaigns, affiliations, motives, exploit code and tools, Response and mitigation strategies, Recommended courses of ac-		

	tion, User screen captures (e.g., error messages or dialog boxes)		
Forensic toolkits and dynamic and/or virtual execution environments	Malware samples, system artifacts (network, file systems, memory)		

Handling requirements for shared threat information

There are many methods to share designations of threat information. The TLP specifies a colour-based set of restrictions that indicate which restrictions apply to a particular record. The Traffic Light Protocol provides a framework for expressing sharing designations.[44]

The TLP is widely used mechanism to classify threat information. Despite the mechanism, it would be necessary identify a mechanism to ensure that the confidentiality of TLP-marked information was not compromised through Freedom of Information (FOI) e.g. National Act on the openness of government activities. It is good to conclude anonymization by National Regulatory Authority (NRA) when sharing information at the European level.

In the TLP, red specifies the most restrictive rule with information sharable only in a particular exchange or meeting, not even within a participant's own organization. TLP consists four colours for different threat levels. The amber, green, and white colour codes specify successively relaxed restrictions. RED It is not for disclosure and it is restricted to participants only. Sources may use RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party´s privacy, reputation or operations if misused. TLP-AMBER illustrates limited disclosure and it is restricted to participants' and organizations. Sources may use TLP-AMBER when information requires support to be effectively acted upon, yet carries risks to privacy or operations if shared outside of the organizations involved. TLP-GREEN is for limited disclosure and it is restricted to the community. Sources may use TLP-GREEN when information is useful for the awareness of all participating organizations but also with peers within the community or sector. TLP-WHITE is not limited. Sources mays use TLP-WHITE when information carries minimal or no foreseeable risk of misuse.

Comparing features of the information sharing models

The main international working groups are Association for Computing Machinery (ACM), National Institute of Standards and Technology (NIST) Institute of Electrical and Electronics Engineers (IEEE) European Telecommunications Standards Institute (ETSI), international Federation for Information Processing (IFIP). NIST Framework is most commonly used of these mentioned above.

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. Table 2 illustrates five different type of models has chosen to more detailed review.

Table 2. Examples of information sharing models.

Organization // Name // System/model or framework type	Main tasks/ features	Special tasks	Major areas of cyber impacts	Instruments
MITRE// CORA // Assessment of cyber operations Based on NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing. MITRE is 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		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Using indicators to 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 (incorporates threat information into its regular security practices).		External Engagement Tools and Data Collection Tracking and Analysis Internal Processes Threat Awareness	Sensors (IDS, HIDS); (IOC) or attack activity such as phishing email addresses, IP addresses and URLs of malicious sites, host-based indicators such as files, registry keys, and process elements.
ENISA// ISAC// Member driven organization model ENISA is a centre of expertise for cyber security in Europe Country-focused ISAC	Sharing knowledge about incidents and cybersecurity. It helps raise the level of cybersecurity in the member organization and prevent/ respond to	ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It provides information	a) a common practice to establish so called “circles of trust.” Some information (e.g. technical details about threats and incidents) can be shared	web portal/platform (following a specific template) and encrypted emails

Sector specific ISAC// Focused on the sectorial level of critical infrastructure or essential/vital sector International ISAC	the incidents which occur (ISAC is a fast and efficient way to get all the knowledge and experience which normally takes a lot of time. ISAC is a good way of networking and meeting people from different organizations. It also provides knowhow)	about threats and incidents. (close cooperation with the industry, public entities get better understanding of the private sector)	widely with all members b) the shared information is more detailed in internal circle c)use of the (TLP) to share information	
ENISA// PPP// Cooperative model	Access to public funds		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
	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 – allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis.			
NIST// Framework// Framework The National Institute of Standards and Technology is part of U.S Department of Commerce	NIST FW targeting on risk management, procedures and privacy preservation aspects. The guidelines included in the ISO/IEC27010 standard, itis oriented toward the protection of the data exchanged in the information sharing process, as well as to the collection, analysis and correlation of cyber incidents in order to obtain an effective mitigation strategy.		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

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.[45] The entire information-sharing mechanism will not work well if the hub is not working well. 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. There must be deeper trust in environment. Environment should be strengthened through face-to-face meetings and individuals who have a long history of personal rapport. 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.

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. The notable problem is that all countries in EU are not full member of NATO. Most of the member countries of European Economic Union belongs to NATO alliance. Organizational aspect does not mean that Finland or Sweden are outsiders in all sectors in this military alliance. Partnership makes it possible to utilize ready-made information sharing networks developed by NATO. It is important to understand the difference between a partnership and a membership. 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." NATO is currently dependent on the cyber defence ability of the United States and the EU has no ability to respond to external cyber threats.

As many politicians and officers has mentioned functionalities between cyber situation centres within European Union are too scattered. Separate functionalities in the member states are not only problem. When the common goal is to im-

prove 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 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.

Conclusions

There is tendency in Europe that private actors are allowed more rights to handle citizens' privacy data. For example, the bank sector has had opportunity to process and handle account data of customers. At the moment, this right is being expanded to other activities. Legislation is not the only factor which affects the chances to completely secure the cyber ecosystem. It is important to notice that information sharing systems or frameworks are useless without features and functionalities. The USA and its public safety cyber defence organizations have ability to combat cyberattacks against vital functions, but also to counterattack. This is one of the most important features in protecting the western world. Cooperation and collaboration in triangle EU-NATO-USA is therefore particularly important. 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 trust organization's functionalities is occasional. What are the organisations, which handle the databases concerning privacy issues and what for they handle it? Where companies and organisations are registered? Does it cause obstacles and can they be overcome when the aim is to catch cyber criminals or find out state level actor utilising cyber or hybrid attacks. The differences between the functionalities and features of information sharing models in USA and NATO versus European Union models for information exchange are converging only if EU develops towards a federal state.

Acknowledgement

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 830943.

References

1 ENISA, "Good Practice Guide – Network Security Information Exchanges," 2009.

2 The Department of Homeland Security (DHS), "Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise," DHS, 2011.

3 Ministry of the Interior of Finland, "National Risk Assessment," Helsinki, 2018.

[4] Secretariat of The Security Committee of Finland, *Finland´s Cyber Security Strategy – Government Resolution* (Helsinki: Ministry of Defence, 2013).

[5] Matthew P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (National Institute of Standards and Technology, NIST, April 16, 2018), https://doi.org/10.6028/NIST.CSWP.04162018.

[6] Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

[7] Victoria Y. Pillitteri and Tanya L. Brewer, *Guidelines for Smart Grid Cybersecurity*, Volume 2, "Privacy and the Smart Grid" (National Institute of Standards and Technology, September 25, 2014), https://doi.org/10.6028/NIST.IR.7628r1.

[8] ENISA, "Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)," European Union Agency for Network and Information Security, 2013.

[9] Latif Ladid, Jart Armin, and Heidi Kivekäs, "Whitepaper: The Finish Electronic Communications Regulator TRAFICOM – A Cybersecurity Reference Model for Europe," Helsinki, SAINT Consortium/Traficom, 2019.

[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," *Official Journal* L 194, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[11] ENISA & ITE, "Information Sharing and Analysis Centers (ISACs) Cooperative Models," European Union Agency for Network and Information Security, 2017.

[12] Greg White and Rick Lipsey, "ISAO SO Product Outline," ISAO Standards Organization, May 2, 2016.

[13] Electrical Technology, "Internet of Things (IOT) and Its Applications in Electrical Power Industry," last update 2016, http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html, accessed August 11, 2016.

[14] National Institute of Standards and Technology, Guide for Conducting Risk Assessments, SP 800-30 Rev. 1, Publication 800-30 (Gaithersburg, MD: U.S. Department of Commerce, 2012), https://doi.org/10.6028/NIST.SP.800-30r1.

[15] *Information Technology — Security Techniques — Information security Management for Inter-sector and Inter-organizational Communications*, ISO/IEC 27010:2015, https://www.iso.org/standard/68427.html.

[16] Christopher Johnson, Mark Badger, David Waltermire, Julie Snyder, and Clem Skorupka, "Guide to Cyber Threat Information Sharing," NIST Special Publication 800-150 (Gaithersburg, MD: National Institute of Standards and Technology, 2016), https://doi.org/10.6028/NIST.SP.800-150.

[17] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[18] Piret Pernik, Jesse Wojtkowiak, and Alex Verschoor-Kirss, *National Cyber Security Organization: United States* (Tallinn: NATO CCD COE, 2016).

[19] Brad Bigelow, "The Topography of Cyberspace and Its Consequences for Operations," *10th International Conference on Cyber Conflict 2018* (Tallinn: NATO CCD COE, 2018).

[20] Bruce J. Bakis and Edward D. Wang, "Building a National Cyber Information-Sharing Ecosystem," MITRE Corporation, 2017.

[21] ENISA, "Good Practice Guide – Network Security Information Exchanges."

[22] ENISA & ITE, "Information Sharing and Analysis Centers (ISACs) Cooperative Models."

[23] NESA, "EP3R 2013 – Position Paper of the EP3R Task Forces on Trusted Information Sharing (TF-TIS)," European Union Agency for Network and Information Security, 2013.

[24] NESA, "Public Private Partnerships (PPP) Cooperative models," European Union Agency for Network and Information Security, 2017.

[25] "Migration and Home Affairs," Information exchange, European Commission, June 17, 2019, https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] European Commission, "Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions," Brussels, European Commission, 2013, https://eur-lex.europa.eu/procedure/EN/202369.

[31] European Commission, "EU-U.S. Privacy Shield: stronger protection for transatlantic data flows," Brussels, 2016.

[32] "NIS Directive," Homepage of European Union Agency for Network and Information Security, https://www.enisa.europa.eu/topics/nis-directive.

[33] Martti Lehto, Jarno Limnéll, Tuomas Kokkomäki, Jouni Pöyhönen, Mirva Salminen, Kyberturvallisuuden strateginen johtaminen Suomessa," Julkaisusarja 28/2018 (Helsinki, Valtioneuvoston kanslia, 2018).

[34] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal* L 119, May 4, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[35] Ibid.

[36] Igor Nai Fovino, Ricardo Neisse, Alessandro Lazari, Gian-Luigi Ruzzante, Nineta Polemi, and Malgorzata Figwer, "European Cybersecurity Centres of Expertise Map – Definitions and Taxonomy," Luxembourg, Publications Office of the European Union, 2018.

[37] Robert K. Yin, *Case Study Research, Design and Methods*, 5 ed. (Thousand Oaks, Sage Publications, 2014).

[38] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[39] Florian Skopik, Giuseppe Settanni, and Roman Fiedler, "A Problem Shared is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing," *Computers and Security* 60 (July 2016): 154-176.

[40] Clement W. Skorupka and Lindsley G. Boiney, "Cyber Operations Rapid Assessment (CORA): A Guide to Best Practices for Threat-Informed Cyber Security Operations," The MITRE Corporation, February 2016, http://www.mitre.org/publications/technical-papers/cyber-operations-rapid-assessment-cora-a-guide-to-best-practices-for.

[41] MITRE, "Cyber Information-Sharing Models: An Overview," MITRE Corporation, 2012, https://www.mitre.org/publications/technical-papers/cyber-informationsharing-models-an-overview.

[42] Johnson, et al., "Guide to Cyber Threat Information Sharing."

[43] Ibid.

[44] Ibid.

[45] MITRE, "Cyber Information-Sharing Models: An Overview."

About the Author

Jussi Simola is a PhD student of cyber security in University of Jyväskylä. His area of expertise includes decision support technologies, situation awareness systems, information security and continuity management. His current research is focused on the effects of the cyber domain on the hybrid emergency response model.