# Enhancing the European Cyber Threat Prevention Mechanism

J Simola

*Laurea University of Applied Sciences*
*RDI Espoo, Finland*
*University of Jyväskylä, Finland*

*Email: simolajussi@gmail.com*

***Abstract:*** *This research will determine how it is possible to implement the national cyber threat prevention system into the EU level Early Warning System. Decision makers have recognized that lack of cooperation between EU member countries affects public safety at the international level. Separate operational functions and procedures between national cyber situation centres create challenges. One main problem is that the European Union does not have a common cyber ecosystem concerning intrusion detection systems for cyber threats. Also, privacy and citizens' security as topics are set against each other. The research will comprise a new database for the ECHO Early Warning System concept.*

**Keywords:** *Information Sharing, Cybersecurity, HAVARO, Privacy, Early Warning*

## Introduction

This paper will comprise a new database for the ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) Early Warning System concept. E-EWS aims at delivering a security operations support tool which enables the members of the ECHO network to coordinate and share information in near real time. Within the E-EWS, partners of ECHO can retain their fully independent management of cyber-sensitive information and related data management. The Early Warning System will work as a parallel part of other mechanisms in the public safety environment. Crucial scientific literature, interviews, and official publications concerning cybersecurity information sharing generate fundamental knowledge to understand the main factors, which separate and combine EU member countries in this environment. The purpose is to support the technical designers of the E-EWS consortium to develop the Early Warning System. Also, interviews of the cybersecurity specialists form crucial sources for the paper.

The HAVARO, organized by TRAFICOM (the Finnish Transport and Communications Agency) and NESA (National Emergency Supply Agency), is one kind of national early warning system, which gathers threat-informed data and produces crucial information concerning the situation of cybersecurity information sharing within critical infrastructure (Ladid, Armin & Kivekäs 2019).

This paper will explore those factors (requirements) which affect the conversion of a national EWS to a common early warning ecosystem at the EU level. Every EU member country has its own system for monitoring and protecting the cyber domain among vital functions. It must be understood

that national systems must find common procedural and governance models in the name of the common good. In addition, privacy-issue-related problems concern the whole cyber ecosystem. The public safety sector will not operate in an isolated dimension without connection to private sector companies. The crucial question is how to combine and share relevant data between stakeholders at the national level and at the international level.

The paper starts with a section introducing the background of challenges concerning critical infrastructure protection and discusses cybersecurity information sharing at the EU level and with the U.S. The next section handles the national HAVARO system and system requirements. The paper concludes with suggestions for a bases of the solution and conclusions about the research area.

## Challenges Concerning Critical Infrastructure Protection

According to the Horizon 2020 work program, disruption in the operation of EU member countries within critical infrastructure may result from hazards and physical or cyber-physical events (European Commission 2019).

Public safety authorities have noticed in Finland that protecting modern infrastructures and vital functions needs not only to protect physical operative functionalities and equipment; they also need the cyber-dimension in their daily routine. It is possible to integrate cyber-threat-informed functionalities of the computer emergency response teams and operative functions of the public safety organizations. These integrated systems are examples of Cyber Physical Systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world (Secretariat of the Security Committee 2019).

In the European Union, there has been a common will to enhance cooperation between public authorities. According to the European Council (2010), Europol collects and exchanges information and facilitates cooperation between law-enforcement authorities in their fight against cross-boarding organized crime and terrorism. Eurojust drives coordination and increases the effectiveness of judicial authorities. Frontex manages operational cooperation at the external borders. The EU operates as the Counterterrorism Coordinator. Several networks have also been established in the fields of training, drugs, crime prevention, corruption, and judicial cooperation in criminal matters (European Council 2010). Solutions are based on common recognition for information sharing and are designed to ease joint investigations and operations. Instruments based on mutual recognition include the European Arrest Warrant and provision for the freezing of assets (European Council 2010). The report is only 10 years old, and only two lines of text have been used to analyse cyber threats.

There are separate local situation centres for emerging situations and emergency response systems, and there are separate cyber-threat functions at the national and EU level. All work mainly without synergy. ICT development projects—for example MARISA, EUCISE, and RAPID—are European-Commission-funded projects that are producing better common situational awareness among EU member countries. The main limitation to implement the RAPID system is related to a lack of cooperation between the EU countries and real-time features of the mechanism. In addition, a lack of leadership causes problems in collaboration (Apuzzo 2019).

One crucial thing is still missing: combined cyber-physical functionalities (Simola & Rajamäki 2017). It is not enough that there are national computer emergency response teams, which only

monitor Internet traffic. In the future, there is a growing need to use proactive or preventive functionalities among public safety organizations.

## Information Sharing at the EU Level and a National Intrusion-Detection System

Shared (cyber) situational awareness is closely related to (cybersecurity) information exchange (Bolstad & Endsley 2000). Bolstad and Endsley (2000) define the development of shared Situational Awareness as consisting of these four factors:

- Shared SA requirements (degree to which team members realize which information is needed by other team members);
- Shared SA devices (communications);
- Shared SA mechanism (shared mental models); and
- Shared SA processes (effective team processes for sharing relevant information).

According to Munk (2018) information interoperability is the joint capability of different actors—such as persons, organizations, and groups—necessary to ensure the exchange and common understanding of the information needed for their success.

The central government of Finland is one of the most important administrative actors that needs correct environment-related cyber situational awareness. When something abnormal occurs, different ministries try to gather and to share the same data from the site of an accident. The common cybersecurity information-sharing procedure enables the government to react to new kinds of threats. There is a need to create a common early warning system with preventive functions. Service producers may be based on public organizations and private companies. One of the most important things is that governance responsibilities of the operational functions should be designated in the future.

In partnership with the National Emergency Supply Agency (NESA), TRAFICOM created the system called HAVARO 1.0 in 2011 (National Cybersecurity Center-FI [NCSC-FI] 2019). It is optional for every Finnish organization to join the system. The information on situation awareness provided by the system increases understanding of the organization´s own and the general state of information security. The system produces information, which makes it possible to alert other players about a detected threat and to develop better tools of detection. The participating organizations are responsible for the costs of equipment needed for their network.

The companies and public administration operators participate in the HAVARO operation voluntarily. The operation of the system is based on the information security threat identifiers coming from different sources. With the help of the identifiers, harmful traffic can be detected from the organization's network traffic. The NCSC-FI receives the information about the anomalies and analyses them. In case of an information security threat, the organization is warned. Based on the information from the HAVARO, the other operators can also be warned about the detected threat. That way, the system helps not only individual organizations, but also helps form a general view of information-security threats against Finnish information networks. TRAFICOM provides the GovHAVARO service for the state administration operators. It completes the information and cybersecurity threat detection of the state administration's Internet traffic. The main problem with HAVARO 1.0 concerns the monitoring ability (Lehto *et al.* 2018). It mainly monitors informa-

tion-security incidents in Internet traffic (KPMG 2013). It is incapable of monitoring the communication of individual user behaviour.

In the future, it is not enough to monitor only the Internet traffic of companies. There should be a wider right to access the organizations' information systems and communication because the Internet of Things (IoT) is changing the way the Artificial Intelligence atmosphere is understood. When electrical and telecommunication cables are placed in the same pipeline, possibilities for vulnerabilities increase.

The HAVARO service is now under development. Instead of being a government service, HAVARO 2.0 will be jointly provided by commercial operators and the NCSC-FI. Some of the events will be processed and reported by information Security Operations Centres (SOC). The objective of the HAVARO 2.0 project is to create the trust network in which the members can exchange information among themselves better than they have before. The HAVARO 2.0 Early Warning System will consist of features of the existing 1.0 system with developed early-warning dimensions. Existing cyber-threat sensor systems need more specialized detection features. Increasing the cyber-threat atmosphere will force stakeholders to develop a better and more efficient system. Separate forensics methods, gathering logs, gathering information, reverse engineering, and analysing risks are not enough in the future. It is crucial to produce added value by combining different data sources and weak threat signals. HAVARO 2.0 will only be complementary to other cybersecurity services.

HAVARO 2.0 will include the GovHavaro feature (Lehto *et al.* 2018). That means that there will be a connection between public organizations and the HAVARO Early Warning System. This information is classified as more confidential, but sector-based sharing requires the sharing of this information to all public safety organizations and to the central government. At the EU level, this information is important to be shared in real time to the stakeholders if threat-information regarding cybersecurity related information to other countries or threat information generates a common risk to vital functions. New stakeholders of the HAVARO 2.0 have contractual relationships with SOCs, not with the NCSC.

## Cybersecurity Information Sharing with the U.S.

There are no fundamental differences in administrative functions between the European Union and the United States. Mainly there are more similarities than differences. Legislation and regulation between the U.S. and the EU are coming closer to each other. The NIS directive in the EU will help to develop next-generation early warning systems.

According to the European Parliament and the Council of the European Union (2016), General Data Protection Regulation (GDPR) 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, if a company is holding private information about an EU citizen to whom it provides services, GDPR applies. It strengthens the rights of private information, access, and the right to be forgotten. The GDPR protects personal data regardless of the technology (automated and manual processing) used. GDPR concerns both unions. The U.S. and the EU have made fundamental agreements to generate a common base for fluent information sharing (European Parliament and the Council of The European Union 2016). Public safety actors, like European law enforcement agencies, need a common situational picture for the cross-boarding tasks so that operational cooperation will be based on a reliable platform.

The European Commission presented the cybersecurity strategy of the European Union in 2013. It set out the EU approach on how to best prevent and to respond to cyber disruptions and attacks as well as emphasized that fundamental rights, democracy, and the rule of law need to be protected in the cyber domain. Cyber resilience is one of the strategic priorities. That means that effective cooperation between public authorities and the private sector is a crucial factor, that the national Network and Information Sharing competent authorities should exchange relevant information with other regulatory bodies.

The information sharing between the EU and the U.S. 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-US Privacy Shield (European Commission 2016). The framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as brings legal clarity for businesses relying on transatlantic data transfers. The EU-US Privacy Shield is based on several principles that govern companies that handle data. They are as follows: 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) the U.S. has given the EU assurance that the access of public authorities for law enforcement and national security are subject to clear oversight mechanisms; c) citizens who think 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 Department of State will ensure that complaints are properly investigated and addressed in a timely manner (European Commission 2016).

According to the U.S. Department of Commerce (2020), the United States has taken a different approach to improving the protection of privacy from that taken by the European Union. The United States uses a sectoral approach that is based on a combination of legislation, regulation, and self-regulation. The approach provides organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union. This mechanism ensures that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when it has been shared to outside of the EU area. The Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles under its statutory authority to foster, promote, and develop international commerce (U.S. Department of Commerce 2020).

## Challenges with the Privacy Shield Agreement

Privacy activists have challenged the Privacy Shield Agreement by arguing that U.S. national security laws did not protect EU citizens from government snooping. On 16 July 2020, the EU Court of Justice made the decision about the adequacy of the protection provided by the EU-US Data Protection Shield by invalidating the agreement (Court of Justice 2020). Despite this decision, the EU Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries is valid. Affected companies will now have to sign 'standard contractual clauses'—non-negotiable legal contracts drawn up by Europe, which are used in other countries besides the U.S. As regards the requirement of judicial protection, the Ombudsperson

mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the U.S. intelligence services. For the above, the Court of Justice declared the European Commission Decision 2016/1250 invalid (Court of Justice 2020).

The purpose of standards is to simplify the work of authorities, to facilitate trade, and to make consumers' everyday lives easier. Standardization helps companies and enterprises to create common rules for information sharing and data handling. The family of 270XX standards provides the bases for the definition and implementation of an Information Security Management System (ISMS). For example, standard ISO/IEC 27010:2015 belongs to an ISO 27000 family and is a key component of trusted information sharing. This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors (International Organisation for Standardisation 27010:2015).

A trusted independent entity would be appointed by the information-sharing community to organise and to support their activities, for example, by providing a source anonymization service (International Organisation for Standardisation 27010:2015).

ISO standard 11179 (2019) provides guidelines for the naming and definition of data elements, as well as information about the metadata captured about data elements (International Organisation for Standardisation 11179-7:2019). Standard 24745 (2011) ensures that any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains; from which identification or contact information of an individual person can be derived; or that is or might be directly or indirectly linked to a natural person be kept private. These are only examples of a wide range of standards that companies must follow. Standardization strengthens product compatibility and safety, protects the citizens, and protects the environment (International Organisation for Standardisation 24745:2011).

## System Requirements

Humans are not as good at processing large volumes of data—quickly and consistently. Flexible autonomy should provide a smooth, simple, seamless transition of functions between the human and the system (Endsley 1988).

National early warning system and information sharing among ECHO EWS partners sets requirements for the basis of the research. Collected materials comes from the scientific literature, interviews of IT specialists, research articles, and official publications.

ECHO EWS will deliver a secure sharing support tool for public-safety personnel to coordinate and to share information in near real-time. It will support information sharing across organizational boundaries and will provide the sharing of general cyber information as a reference library. It will also ensure secure connection management from clients accessing the E-EWS. It will combine different kinds of functions required in the management of information-sharing functions, including sector-specific cyber-sensitive data. All participants (administrative actors, EU countries, companies, cyber situational centres, and public safety authorities) set requirements for developing

ECHO system governance and the Early Warning System. The big challenge is the diversity of stakeholders included in the ECHO. Therefore, system requirements cannot place too many challenging barriers to the development of the E-EWS.

When the aim is to share essential information between stakeholders as soon as possible, information sharing must be automatized. AIS (Automatic Identification System) utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication. STIX is a language and serialization format that enables organizations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner. Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange cyber threat intelligence (CTI) over the HTTPS (Department of Homeland Security [DHS] 2019). Echo EWS system requirements are based on requirements concerning governance model and Echo Federated Cyber Range.

Bromander, Muller and Jøsang (2020) have criticized the use of STIX because of various ways of representing the same information, the possibility of automatic consumption, and the fact that computer-based analysis becomes limited. If a computer cannot identify information because the information type is not normalized, 'Big Data'-style analysis is not possible; therefore, manual work is needed to correct and to analyse the data Also lack of standardization concerning all relevant information poses a problem for automation. Bromander, Muller and Jøsang (2020) argue that while many claim to use STIX, in most cases it is not used as a standardized way of sharing CTI suitable for automation. The criticism is justified and seems to concern large companies. However, there are currently no well-developed alternative good solutions.

## Suggestion for a Basis of the Solution

This section describes the findings and suggested basis of a solution for national information sharing. First, the information-sharing architecture in the U.S. will be addressed. After that, methodologies for the indicator sharing and possible features for the early warning system will be introduced.

## Information-sharing architecture in the U.S.

NCSC-FI (National Cybersecurity Center) and NESA (The National Emergency Supply Agency) have made an industry-specific classification for sharing cyber-threat information. The classification is demonstrated as follows: VIRT, public organizations, defense industry, energy sector, finance, industry automation, chemical and process industry, logistics sector, food industry, health sector, industrial companies, equipment and product manufacturers, ICT, media industry, security consultants, security researches, CERT-actors. Despite the classification, there is a need to expand collaboration within public and private actors. NESA, as a partner of TRAFICOM, is responsible for vital functions of society in Finland (NCSC-FI 2017). This classification mainly follows the European model, but also follows the sector-based classification in the U.S.

As mentioned above, the information-sharing model used in the U.S. is possible to replicate in the European Union. There are more similarities than differences. The simple picture in **Figure 1**, below, shows how information is shared. Automated information (indicator) sharing is mainly based on centralized ISACs, which consist of all actors of the specific sector. As illustrated in **Figure 1**, below, sector-based Information Sharing and Analysis Centers (ISACs) are one kind of government-prompted, industry-centric sharing model. Centers are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between

government and industry (ENISA & ITE 2017). Finland uses a similar national level structure of information sharing. It is based on the classification of different sectors of critical infrastructure. There are 16 levels of critical infrastructure used in the U.S. The same sector-specific frame is almost in use everywhere in western countries (White House 2013a; 2013b).

Open Communities and Platforms are open-source sharing platforms. For example, STIX indicators and open-source intelligence feeds are this kind of format. The Malware Information Sharing Platform (MISP) is a free, open-source platform developed by researchers from the Computer Incident Response Center of Luxemburg, the Belgian military, and NATO. For example, Interpol uses the Malware Information Sharing Platform (GitHub 2019; OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a).

## HAVARO as a part of the European Early Warning System

There are several factors that are important to notice if the purpose is to integrate the national Early Warning System to the common European Union level Early Warning System. First, the use of cloud services is not a secure way to store and gather threat-informed data. When customers of the early warning solution are connected to the system from all around Europe, using cloud-only service solutions is not secure because cyberattacks against virtual machines may jam the whole system. Therefore, the authors recommend using a centralized main server that produces services to EWS stakeholders. This sharing model requires using local (national) E-EWS servers where ECHO-EWS is connected This is one kind of hybrid model, but the model is a secure part of the architecture, which allows sharing trust-level information. It is important that, for example, the National Bureau of Investigation have the ability to gather and to share trust-level information concerning vital functions of society and have the ability to be connected in the Early Warning System. It is relevant that the early warning data is shared from the central server to the affected sectors. International researchers recommend using a controlled information-sharing model, where national public safety actors share relevant data to stakeholders via a centralized center (EWS Center [Department of Homeland Security]) as **Figure 1** illustrates.

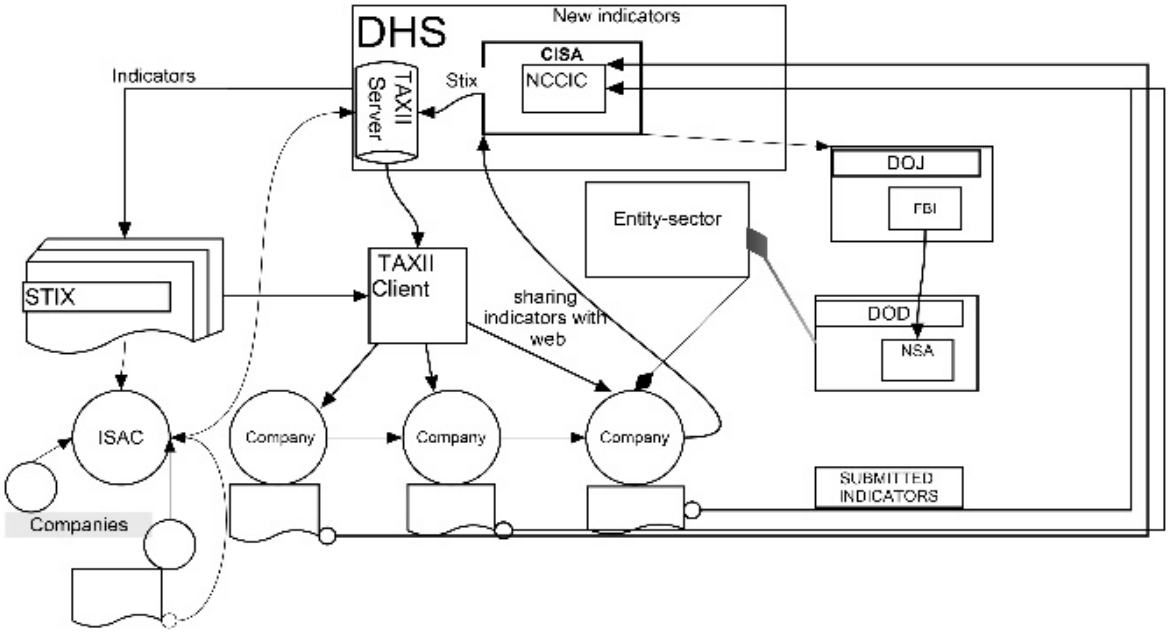


**Figure 1:** Cyber-information sharing model in the U.S.

Two-way models also allow public safety organizations to use gathered information for the prevention of hybrid threats before the domino effect is caused by two or more separate phenomena. It is important that cross-boarding cooperation work directly and instantly. Echo EWS will not work as a separate system but plays a crucial and parallel part in wider mechanisms, including the European-level situational awareness system of NATO. All Echo partners must understand that common language means in a wider manner—for example, taxonomies, techniques, procedures, and common ways to respond and act.

The U.S. Department of Homeland Security uses a system called Automated Indicator Sharing (AIS). AIS participants may connect to a national early warning system in the National Cybersecurity Center (NCSC) that allows also bidirectional sharing of cyber threat indicators. A server housed at each stakeholder´s (community) location allows the stakeholder to exchange indicators with the National Cybersecurity Center (NCCC) as **Figure 1** illustrates. Participants receive and can share DHS-developed indicators that they have observed in their own network defence efforts, which the national cyber situation centre will then share back out to all AIS participants. Stakeholders who share indicators through AIS will not be identified as the source of those indicators to other participants unless they consent to the disclosure of their identity. Senders are anonymous unless they want NCSC to share their identity (Hernandez-Ardieta, Tapiador & Suarez-Tangil 2013). Official cyber-security partners will vet the indicators they receive through AIS.

The government also needs useful information about indicators and other threat-informed data. Therefore, local NCSC should share at least weekly reports to the government situation centre. AIS utilizes the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication. STIX is a language and serialization format that enables organizations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner. Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange cyber threat intelligence (CTI) over the HTTPS (Department of Homeland Security 2019).

Collection-based communications indicate that a single TAXII client is making a request to a TAXII server and the TAXII Server carries out that request with information from a database. A TAXII channel in TAXII Server enables TAXII clients to exchange information with other TAXII clients in a publish-subscribe model. TAXII clients can push messages to Channels and Subscribe to Channels to receive published messages. A TAXII Server may host multiple channels per API root (MITRE 2018; OASIS Cyber Threat Intelligence [CTI] TC, DHS [CS&C] 2017b). TAXII is the main transport mechanism for Cyber Threat Information (CTI) represented in STIX. Stakeholders may share indicators with NCSC through an ISAC or an ISAO without being a TAXII client.

According to the Department of Homeland Security (2019) Cyber Threat Information is any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor.

There are a wide range of the information-sharing methodologies and systems in law enforcement. For example, the main approach of the Europol Information System (EIS) is to be the reference system for offenses, individuals involved, and other related data to support EU member states, Europol, and its cooperation partners in their fight against organized cybercrime, terrorism, and

other forms of serious crime. For example, the European Cybercrime Centre (EC3), as a part of Europol, uses an open source based MISP platform (ENISA 2017). Malware Information Sharing Platform (MISP) is a tool for information sharing about malware samples and related malicious campaigns related to specific malware variants. It offers architectural flexibility and allows the use of a centralized platform (for example, CIRCL and FIRST instances), but also as a decentralized (peer-to-peer) platform.

Europol´s SIENA is a VPN (Virtual Private Network) designed to enable a swift, secure, and user-friendly exchange of operational and strategic crime-related information and intelligence between member states, Europol, law enforcement cooperation partners, and public safety organizations (EUROPOL 2019).

Databases of the Schengen Information System (SIS) and networks have also been established for the exchange of information on criminal records, on combating hooliganism, on missing persons or stolen vehicles, and on visas which have been issued or refused. DNA and fingerprint data help put a name to anonymous criminals who left crime scenes. EU legal instruments facilitate operational cooperation between member states, such as the setting up of collaborative investigation teams and the organizing of joint operations (European Council 2010).

Sharing digital information between stakeholders may include Common Vulnerabilities and Exposures (CVE) or CVE-ID and CVEs that include a list of common identifiers for publicly known cybersecurity vulnerabilities. For example, the HAVARO EWS solution exploits identifiers to detect threats. CVE Numbering Authorities (CNAs) are authorized organizations which assign CVE IDs to vulnerabilities affecting products within their distinct agreed-upon scope for inclusion in first-time public announcements of new vulnerabilities (MITRE Corporation 2019a). MITRE Corporation (2019b) CVE Identifiers are unique, common identifiers for publicly known information security vulnerabilities (MITRE Corporation 2019b).

The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management. The NVD consists of databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics (NIST 2019).

In the CVE list feeds, NVD and CVE entries provide enhanced data for each entry—such as fix information, severity scores, and impact ratings. NVD also supplies advanced searching features (MITRE Corporation 2019a; 2019b).

Digital Forensics XML (DFXML) is an XML language. DFXML improves composability by providing a language for describing forensic processes (for example, cryptographic hashing), forensic work products (for example, the location of files on a hard drive), and metadata (for example, file names and timestamps) (Garfinkel 2012).

According to Garfinkel (2012), the Digital Forensics XML toolset is intended to represent the following types of forensic data:

- Metadata describing the source disk image, file, or other input information.

- Detailed information about the forensic tool that did the processing (for example, the program name, where the program was compiled, and linked libraries).
- The state of the computer on which the processing was performed (for example, the name of the computer, the time that the program was run, the dynamic libraries that were used).
- The evidence or information that was extracted (how it was extracted and where it was physically located); cryptographic hash values of specific byte sequences; operating-system-specific information useful for forensic analysis (Garfinkel 2012).

## Conclusion

The fight against hybrid threats means not only preventing functions against cyberattacks, but also identifying, tracing, and prosecuting a criminal/criminal group. This means even multifunctional integration where existing intrusion detection/prevention systems complement new solutions in the future.

There are no essential barriers to increase collaboration in organizational, tactical, strategical, and technical levels between national CERTs, NATO Computer Incident Response Capability (NCIRC), and EU Computer Emergency Response Team (CERT-EU). Common E-EWS solution would create an effective way to respond to cross-boarding hybrid thread situations. All major companies whose businesses are involved with the vital functions of society should be connected to an early warning system.

The future HAVARO 2.0 that is under development reflects a tendency to develop early warning functions at the national level. However, this is not enough. Critical information must be able to share between EU member countries because several enterprises operate at the international level. Cross-border cyber threats force countries to exchange critical information within EU member countries and between EU and other western states. That means cyber risks have become common challenges.

Operative public safety functions require quicker response or even prediction. HAVARO 2.0 should utilize the Artificial Intelligence (AI) dimension to detect threats. It is not possible to design next-generation early warning information systems without machine learning as part of the Artificial Intelligence (AI) functionalities because the early warning system requires predictive features. Artificial Intelligence functionalities enable entities to exploit difference databases and produce characterized data more effectively than a human can; it may also come to a conclusion by learning from input information. In addition, AI can make a decision without human interaction. This means also that not every ECHO participant has the same potentiality or opportunity to develop national system architecture. International cyber-physical dimension of threats sets requirements, what should be the minimum cybersecurity level or requirements of cyber situational centers at the national level. Framework for the local, national, and international information sharing should follow the same principles in each EU member country. **Figure 2**, below, illustrates the simple formation of cybersecurity information sharing between countries in which HAVARO 2.0 may join. This example consists of separate national sub-hubs and one centralized hub. Information-Sharing participants do not exchange information with each other. All threat-informed data is shared via a hub.

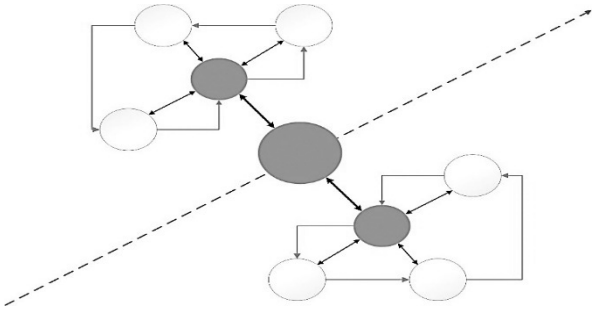

**Figure 2:** Connection between sub-hubs

Therefore, ISAC based national sectorial classification is the optimal way to share classified information as **Figure 3** illustrates.

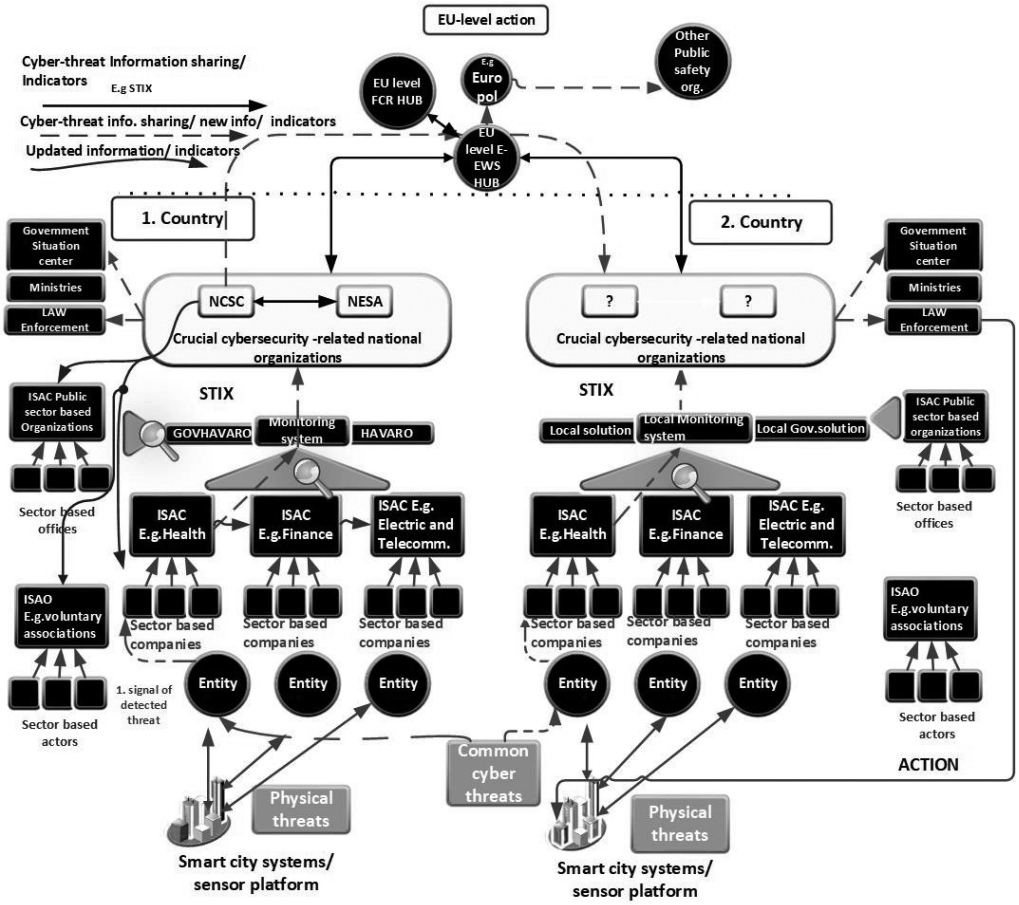


**Figure 3:** Proposed E-EWS information-sharing model

**Figure 3** demonstrates information-sharing relationships and organizational structures concerning information sharing within a centralized hub system (countries, companies, public safety organizations, and other actors). In country number 1 (Finland), identifiers of the national Early Warning System (for example, HAVARO) detect a weak signal of cyberthreat concerning Internet traffic in a multinational enterprise. The national cybersecurity centre of country 2 has not noticed a cyberthreat activity. Automated Information Sharing functionalities produces crucial data for the central EWS hub, which shares relevant information in near real-time to the situation centres (CERT or

CIRT team). Sensitive data will be shared directly to the international public safety organizations and/or to the governments which are associated with the cyberthreat. NCSC of Finland uses a parallel subsystem for public organizations; HAVARO consists of separate early warnings solutions named "GovHavaro" for all public organizations.

Participants do not need to share information directly with each other, but there is a need to establish sector-specific communities—for example, ISAC and ISAO—that collect crucial information concerning the targeted sector of the critical infrastructure. This cybersecurity information is monitored and handled by national CERT or CIRT, and cybersecurity centres will share all new indicators between stakeholders (ISACs). All law enforcement-related information will be shared directly via EWS hub to the public safety authorities, such as EUROPOL or INTERPOL. Centralized EWS hub and sub-hubs are the simplest option for the national Finnish Early Warning System. On the other hand, a big challenge will be who maintains the central hub, and what its governance model would be.

Criticism concerning the use of STIX is justified, as mentioned above, and the problem needs to be rectified. More detailed guidelines, methods, standardization, and compliance with the law create a better operating environment to take advantage of automated indicator exchange.

Despite the invalidated privacy shield decision of the EU Court of Justice, there is a need to strengthen and to be aware of hybrid threats in a wider perspective. Privacy issues are important to protect. It is possible that the content of the privacy shield agreement needs to be changed. The agreement is significant in terms of commerce. Companies will now have to sign 'standard contractual clauses': non-negotiable legal contracts drawn up by Europe, which are used in other countries besides the U.S. (Court of Justice 2020).

## References

Apuzzo, M 2019, 'Europe built a system to fight Russian meddling. It is struggling', *The New York Times*, viewed 1 November 2019, <https://www.nytimes.com/2019/07/06/world/europe/europe-russian-disinformation-propaganda-elections.html->.

Bolstad, C & Endsley, M 2000, 'The effect of task load and shared displays on team situation awareness, *The 14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA, US.

Bromander S, Muller, EM & Jøsang A 2020, 'Examining the "known truths" in cyber threat intelligence – The case of STIX', *Proceedings of the 16th International Conference on Cyber Warfare and Security*, Old Dominion University, Norfolk, VA, US, pp. 493-502.

Court of Justice of the European Union 2020, 'The Court of Justice invalidates decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield', Press release No 91/20, 16 July , viewed 1 June 2020 <https://curia.europa.eu/jcms/jcms/p1_3117870/en/>.

Department of Homeland Security (DHS) 2019, 'Automated Indicator Sharing (AIS)', viewed 1 June 2019, <https://www.us-cert.gov/ais>.

Endsley, MR 1988, 'Design and evaluation for situation awareness enhancement', *Proceedings of the Human Factors Society 32nd Annual Meeting*, pp. 97-101.

ENISA 2017, 'Tools and methodologies to support cooperation between CSIRTs and law enforcement version 1.0' November, Heraklion, GR,

——& ITE 2017, 'Information sharing and analysis centres (ISACs) cooperative models', Heraklion, GR.

European Commission 2013, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,' viewed 3 June 2020, Brussels, BE, < https://eur-lex.europa.eu/procedure/EN/2023 69>.

——2016, 'EU-U.S. Privacy Shield: Stronger protection for transatlantic data flows', Brussels, BE.

——2019, '14. Secure societies: Protecting freedom and security of Europe and its citizens', *Horizon 2020 - Work Programme 2018-2020*.

European Council 2010, 'Internal security strategy for the European Union towards a European security model', General Secretariat of the Council, European Union, Brussels, BE.

European Parliament and the Council of The European Union 2016, 'Regulation (EU) 2016/679 of the 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, 4 May, viewed 1 August 2019, <https://eurlex.europa.eu/eli/reg/2016/679/oj>.

EUROPOL 2019, 'Secure Information Exchange Network Application (SIENA)'. viewed 1 August 2019, <https://www.europol.europa.eu/activities-services/services-support/information-exchange/secure-information-exchange-network-application-siena>.

Garfinkel, S 2012, 'Digital forensics XML and the DFXML toolset', *Digital Investigation*, vol. 8, pp. 161-74.

GitHub 2019, 'Support your workflow with lightweight tools and features', viewed 7 July 2019, <https://github.com/MISP/MISP-Taxii-Server>.

Hernandez-Ardieta, JL, Tapiador, JE & Suarez-Tangil, G 2013, 'Information sharing models to cooperative cyber defence', *Proceedings of the 5th IEEE International Conference on Cyber Conflict (CyCon) 2013*, pp. 1-28.

International Organization for Standardization 2011, 'Information technology — Security techniques — Biometric information protection ISO/IEC 24745:2011', viewed 5 July 2020, <https://www.iso.org/standard/52946.html>.

——2015, 'Security techniques information security management for inter-sector and inter-organizational communications', ISO/IEC 27010:2015, viewed 5 July 2020, <https://www.iso.org/standard/68427.html>.

——2019, 'Metadata registries (MDR) — Part 7: Metamodel for data set registration', ISO/IEC 11179-7:2019, viewed 5 July 2020, < https://www.iso.org/standard/68766.html>.

KPMG 2013, 'IDS:N käyttöönotto herättää todellisuuteen', viewed 5 July 2019, <https://www.hackingthroughcomplexity.fi/2013/04/idsn-kayttoonotto-herattaa.html>.

Ladid, L, Armin, J & Kivekäs H 2019, 'The Finish electronic communications regulator TRAFICOM - A cybersecurity reference model for Europe', SAINT Consortium/ TRAFICOM, Helsinki, FI.

Lehto, M, Limnéll, J, Kokkomäki, T, Pöyhönen, J & Salminen, M 2018, '*Kyberturvallisuuden strateginen johtaminen Suomessa* No. 28', *Valtioneuvoston kanslia*, Helsinki, FI.

MITRE Corporation 2018, 'Trusted Automated eXchange of Indicator Information - TAXII™ enabling cyber threat information exchange', U.S Government.

——2019a, 'Common vulnerabilities and exposures', viewed 6 July 2020, <https://cve.mitre.org/cve/cna.html>.

——2019b, 'CVE-details', viewed 6 June 2020, <https://www.cvedetails.com/cve-help.php>.

Munk, S 2018, 'Interoperability services supporting information exchange between cybersecurity organisations', *Academic and Applied Research in Military and Public Management Science*, vol. 17, no. 3, pp. 131-48.

National Cybersecurity Center-Finland (NCSC-FI) 2017, '*Viestintäviraston kyberturvallisuuskeskuksen palvelut*', Brochure Cybersecurity services of the NCSC-FI. Helsinki: TRAFICOM.

——2019, 'Havaro service and FAQ', viewed 5 July 2020, <https://www.kyberturvallisuuskeskus.fi/en/havaro-service>.

NIST 2019, 'National vulnerability database - General information', viewed 1 September 2019, <https://nvd.nist.gov/general>.

OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a, 'STIX™ version 2.0. Part 2: STIX objects No. stix-v2.0-wd03-part2-stix-objects) OASIS open'.

——2017b, TAXII™ version 2.0. 'Committee specification 01 No. taxii-v2.0-cs01) OASIS Open'.

Secretariat of the Security Committee 2019, 'Finland´s cybersecurity strategy - Government resolution', Ministry of Defense, Helsinki, FI.

Simola, J & Rajamäki, J 2017, 'Hybrid emergency response model: Improving cyber situational awareness', *Proceedings of the 16th European Conference on Cyber Warfare and Security*, University, College, Dublin, IE, pp. 442-51.

United States Department of Commerce 2020, 'The Privacy Shield framework in the United States', viewed 6 July 2020, <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text>.

White House 2013a, 'Critical infrastructure security and resilience', Presidential Policy Directive, USC.

——2013b, 'Federal register - Improving critical infrastructure cybersecurity, Part III - Executive Order 1363', vol. 77, USC.