National Cyber Threat Prevention Mechanism as a part of the E-EWS

Jussi Simola [1,2] and Martti J. Lehto [2]
[1]Laurea University of Applied Sciences, RDI Espoo, Finland
[2]University of Jyväskylä, Finland
jussi.simola@laurea.fi; juhemisi@student.jyu.fi
martti.j.lehto@jyu.fi
DOI: 10.34190/ICCWS.20.106

Abstract: The research will find out feature-based functionalities concerning the national cybersecurity system HAVARO and how the system is possible to implement to the EU level early warning system. The research based on interviews, official materials concerning the HAVARO information sharing system, scientific literature and other official published documents. The European level decision-makers have recognized that lack of cooperation between EU member countries effects to completely public safety atmosphere. The only problem does not consist of separate operational functions and procedures between national Cyber situation centers. One main problem is that the European Union does not have a common cyber-ecosystem concerning intrusion detection systems for cyber-threats. The research will comprise a new database for the common Early Warning System concept. European EWS aims at delivering a security operations support tool enabling the members of the network to coordinate and share information in near real-time. Despite the development of the common EWS, partners can retain their fully independent management of cyber-sensitive information and related data management.

Keywords: information sharing, HAVARO, cybersecurity, early warning

1. Introduction

The aim of the research is to find out crucial national elements for the common Early-Warning system at the EU level. In this context, the elements mean functionalities and procedures but also technical solutions concerning Cybersecurity information sharing.

This research will comprise a 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. 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 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 and find essential literary material for the development work of the Early Warning System.

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 gather threat informed data and produce crucial information concerning the situation of cybersecurity information sharing within critical infrastructure (Ladid & al., 2019).

The research will find out the pros and cons of the HAVARO system and what are those factors (requirements), which effect for implementing national EWS system to common early warning ecosystem in 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 into an isolated dimension, without connection to private sector companies.

The research questions are: What are the main features of the cybersecurity information sharing model called HAVARO and how the early warning solution HAVARO and GovHAVARO (for public organizations) can be integrated and implement to the ECHO Early warning system solution? Following sub-questions are discussed: How to create connection between existing procedures and a new generation system with preventive or

(predictive) cyber functions concerning cyber-information sharing? How to combine and share relevant data between stakeholders at the national level and at the international level? It is important to take into account that private-public, private-private, public-private and public-public features must be included in multidirectional information sharing functions?

The contest of the research is divided as follows. Section 2 handles the background of the research. Section 3 handles the national HAVARO system. Section 4 presents the research approach and methods. Section 5 presents the findings. Section 6 handles conclusions about the research area.

2. Background

2.1 Specific challenges concerning Critical Infrastructure Protection

According to 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).

Several public safety organizations have noticed in Finland, that protecting modern infrastructures and vital functions need not only physical operative functionalities and equipment, they also need cyber-dimension in their daily routine. It is possible to integrate cyber-threat informed functionalities of the e.g., 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, 2013). Therefore, it is important to create a system, which gathers cyber-threat-related information to all participants.

There are separate local situation centers for emerging situations, emergency response systems, separate cyber threat functions at the national and EU level. All works mainly without synergy. Ongoing ICT development projects e.g., MARISA and EUCISE are European Commission funded projects at the EU level, which are producing better common situational awareness between EU member countries. There are also almost implemented EU -funded systems and mechanisms like RAPID. 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, lack of leadership causes problems in collaboration (Apuzzo, 2019).

One crucial thing is still missing; combined cyber-physical functionalities (Simola & Rajamäki, 2017). ECHO designers will develop the early warning mechanism, which reacts before any cyber or hybrid-threats will occur. It is not enough, that we have 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.

3. National intrusion detection system HAVARO and Cybersecurity information sharing at EU level

Central Government of Finland is one of the most important administrative actor, which need correct environment-related cyber situational awareness. When something strange or abnormal occurs, different ministries try to gather and share the same data from the site of an accident. The common cybersecurity information sharing procedure enables to react against new kinds of threats. There is a need to create common Early Warning System with preventive functions. Service-producers may base on both, public organizations or private companies. One of the most important thing is governance responsibilities of the operational functions, therefor the responsible organization should be designated in the future.

3.1 Obstacles in the detection system HAVARO 1.0

TRAFICOM (the early name was FICORA) has created in partnership with the National Emergency Supply Agency (NESA) the system called HAVARO in 2011 (NCSC-FI, 2019). It is optional for every Finnish organization to join the HAVARO system. The information on situation awareness provided by the system increases understanding of the organization´s own and general state of information security. The system produces information, which makes it possible to alert other players about a detect threat and 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 or anomalous traffic can be detected from the organization's network traffic. The National Cybersecurity Center (NCSC-FI) receives the information about the anomalies and analyses them. In case of an information security threat, the organization is warned about it. Based on the information got from the HAVARO, also the other operators can be warned about the detected threat. That way, the system helps not only individual organizations but also in forming a general view about the information security threats against Finnish information networks. TRAFICOM provides the GovHAVARO service for the state administration operators. It completes the information and cyber security threat detection of the state administration's Internet traffic.

The main problem about the HAVARO 1.0 concerns the monitoring ability (Lehto, Limnéll, Kokkomäki, Pöyhönen, & Salminen, 2018). It mainly monitors information security incidents only in internet traffic (KPMG, 2013) as fig. Figure 1 Illustrates.

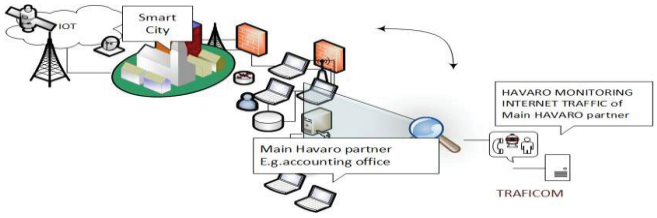

Figure 1: Havaro Early Warning System in enterprise-level

It is incapable of monitoring the communication of individual user behaviour. In the near future, it is not enough to monitor only 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 our way of understanding the Artificial Intelligence atmosphere. When the combined electrical and telecommunication cable is placed on the same place possibilities for the vulnerabilities increases.

TRAFICOM and NESA have increased cooperation within the cyber entity. It is important that NESA operate closely within sector-based cybersecurity, because the agencies, departments, and government of the USA use also sector-based cyber-threat awareness. Deeper possibilities to share information between the stakeholders are key factors when the aim is to enhance common situational awareness.

3.2 HAVARO 2.0

Now the HAVARO service is under development. The foundation of the operation will be the Havaro 2.0 system on the development work of which an agreement with Reaktor Oy was made in September 2018. 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 centers (SOC).

The objective of the HAVARO 2.0 project is to create the trust network in which the members can change information better than before among themselves. Next-generation 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 forcing to develop a better and more efficient system. Separate forensics methods, gathering logs, gathering information, reverse engineering and analyzing risks are not enough in the future. It's crucial to produce added value by combining different data sources and weak threat signals.

HAVARO 2.0 consists also GovHavaro feature (Lehto et al., 2018). That means the connection between public organizations and 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 central government. At the EU level this information is important to be shared in real-time to the stakeholders if threat-information regarding cybersecurity relate information to other countries or threat information generates a common risk to vital functions. Therefor description of the HAVARO 2.0 software development has changed. HAVARO 2.O will process various phenomena much more extensively than HAVARO 1.0. New stakeholders of the HAVARO 2.0 have contractual relationships with SOCs, not with the NCSC.

3.3 Description of the HAVARO 2.0 software development

According to (TED, 2019) the description of the HAVARO 2.0 software development has changed. HAVARO 2.0 software development work is divided as follows:

1. Development of a network monitoring device (sensor);
2. a portal providing an interface for service centers and users;
3. An interface serving as a service bus between sensors, central system, and external systems;
4. A repository where HAVARO 2.0 information is stored.

Developers are required to have knowledge of Python programming language, open-source security software (including Snort, Suricata, and NFDump) and programming languages and technologies used in portals and user interfaces. System development requires experience in service design and usability design, as well as testing and automated software distribution technologies and management (e.g. Puppet or similar). Those who are working on the development of the new system require proactivity in following new cybersecurity and cybersecurity trends and solutions (TED, 2019).

3.4 Cybersecurity Information-sharing with the USA

What are the 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 USA and the EU are coming closer to each other. NIS directive in the EU will help to develop next-generation early warning systems. GDPR concerns both unions. USA and EU have made quite fundamental agreements to generate a common base for fluent information sharing (European Commission 2016). Public safety actors like European law enforcement agencies need a common shared situational picture for the cross-boarding tasks in a way that operational co-operation be based on a reliable platform.

4. Research approach and research methodology

According to (Nunamaker, Minder Chen & Purdin, 1991) the multi methodical approach consists of four case study research strategies: theory building, experimentation, observation and systems development. The research-based on systematic analysis of gathered data.

Gathered data consist of source material from academic literature and official publications. This research-based on Yin´s case study methodology (Yin, 2014). This research defines how to share cybersecurity information among ECHO stakeholders (including national and international level) and how to enhance emergency response in the case of the hybrid incident? 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 human and the system (Endsley, 1988).

National Early warning system and information sharing among ECHO EWS partners sets requirements for the base of the research. Collected materials based on scientific literature, interviews of IT specialists, research articles and official publications. The main research question of the research is: “What are the main features of the cybersecurity information sharing model called HAVARO and how the early warning solution HAVARO and GovHAVARO (for public organizations) can be integrated and implemented to the ECHO Early warning system solution.

4.1 System requirements

ECHO EWS will deliver a secure sharing support tool for public safety personnel to coordinate and share information in near real-time. It will support information sharing across organizational boundaries and provide the sharing of both 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 centers, and public safety authorities) set requirements for developing ECHO system governance and the Early Warning System. The big challenge comprises the diversity of stakeholders included in the ECHO. Therefor system requirements cannot place too 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 (DHS, 2019). Echo EWS system requirements based on requirements concerning governance model and Echo Federated Cyber Range.

4.2 Shared situational awareness between Cyber Emeregency Rerponse Teams

Shared (cyber) Situational Awareness is closely related to (cybersecurity) information exchange (Bolstad & Endsley, 2000). Bolstad and Endsley (2000) define that the development of shared Situational Awareness consists of four factors as follows:

- Shared SA requirements (team members degree to understand 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) cooperation between cybersecurity organizations based on the effective and efficient exchange of information. Information interoperability is the joint capability of different actors like persons, organizations, and groups necessary to ensure the exchange and common understanding of the information needed for their successful (Munk, 2018).

5. Findings

5.1 Information-sharing architecture in the USA

NCSC-FI (National Cybersecurity Center) and NESA (The National Emergency Supply Agency) have made industry-specific classification for sharing cyber-threat information. The classification is demonstrated as follow: 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 follows mainly European level model, but also sector-based classification in The USA.

As mentioned above information-sharing model used in the USA is possible to replicate in the European Union level. There are more similarities than differences. The simple picture below shows how information is shared. Automated information (indicator) sharing mainly based on centralized ISACs, which consists of all actors of the specific sector Figure 2 illustrates. 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). Almost similar national level structure of information sharing is almost in use in Finland. It based on the classification of different sectors of critical infrastructure. There are 16 levels of critical infrastructure used in the USA. The same sector-specific frame is almost in use everywhere in western countries (The White House, 2013a; The White House, 2013b).

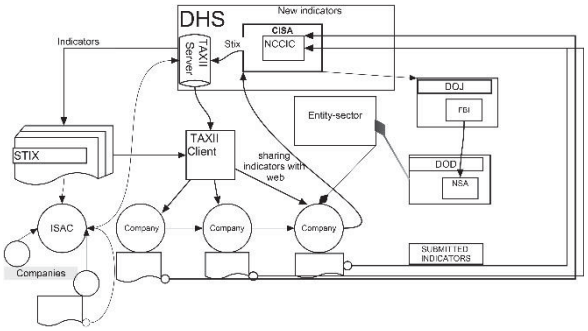

Figure 2: Cyber-information sharing model in the USA

Open Communities and Platforms are open-source sharing platforms. E.g., 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. E.g., Interpol uses The Malware Information Sharing Platform (GitHub, 2019; OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C), 2017a).

5.2 Havaro as a part of the European Early Warning System

There are several factors, which are important to notice, if the purpose is to integrate the national early warning system to the common European Union level early warning system. Firstly, 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 the EUROPE, it is not a secure way to use only cloud service solutions because cyber-attack against virtual machines may jam the whole system. Therefore, our research recommend 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 consists also secure part of the architecture, which allows sharing trust level information. It is important that e.g., for the National Bureau of Investigation have capability to gather and share trust level information concerning vital functions of society and have possibility 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 researches recommends to use controlled information-sharing model where national public safety actor share relevant data to stakeholders via a centralized center (EWS center (DHS)) as Figure 2. illustrates.

Two-way model allows also public safety organizations to use gathered information for the prevention against hybrid threats before separate phenomena illustrates as a domino effect. It is important that cross-boarding cooperation work directly and instantly. Echo EWS will not work as a separate system but 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 e.g. taxonomies, techniques, procedures and common ways to respond and act.

5.3 Automated Indicator Sharing

The U.S Department of Homeland Security uses a system called Automated Indicator Sharing (AIS). Automated Indicator Sharing (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 them to exchange indicators with the National Cybersecurity Center (NCCC) as fig. 2. illustrates participants receive and can share DHS-developed indicators they have observed in their own network defense efforts, which national cyber situation center 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 affirmatively consent to the disclosure of their identity. Senders are anonymous unless they want NCSC to share it (Hernandez-Ardieta & al., 2013). Official cyber-security partner as NCSC will vet the indicators they receive through AIS. The main goal is to share as many indicators as possible as quickly as possible. The Government also need useful information about indicators and other threat-informed data. Therefor local NCSC should share at least weekly reports to the government situation center.

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 (The Department of Homeland Security (DHS), 2019).

Collection based communications mean the situation when a single TAXII client makes 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 represented in STIX. Stakeholders may share indicators with NCSC through an ISAC or an ISAO without TAXII client.

5.4 Formation of cyber threat information

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. Major types of threat information include the following:

- Indicators of Compromise (IoC´s) are technical observables. Indicators can be used to detect and defend against threats. Indicators may consist the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message (The Department of Homeland Security, 2019).
- TTPs: Tactics, techniques, and procedures could describe an actor's tendency to use a specific malware, attack tool, or delivery mechanism. (The Department of Homeland Security, 2019).
- Security alerts, also known as advisories, bulletins, and vulnerability notes, are brief and usually readable technical notifications regarding current vulnerabilities, etc. Security alerts originate from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centers (ISACs), the National Vulnerability Database (NVD), Product Security Incident Response Teams (PSIRTs), commercial security service providers, and security researchers (The Department of Homeland Security, 2019).
- Threat intelligence reports are generally prose documents that describe TTPs, actors, types of systems and targeted information and other threat-related information that provides greater situational awareness to an organization (The Department of Homeland Security, 2019).

5.5 Information sharing methodologies in Law Enforcement

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. E.g., the European Cybercrime Centre (EC3) as a part of Europol uses an open source-based MISP platform (ENISA, 2017). Malware Information Sharing Platform (MIPS) is a tool for information sharing about malware samples and related malicious campaigns related to specific malware variants. It offers architectural flexibility allowing the utilization as a centralized platform (e.g. 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).

5.5.1 Shared digital library among EWS stakeholders

Common Vulnerabilities and Exposures (CVE) or (CVE-ID and CVEs) comprises a list of common identifiers for publicly known cybersecurity vulnerabilities. E.g., the Havaro EWS solution exploits identifiers to detecting 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). Information security product or service vendors and researchers use CVE Identifiers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers. MITRE Corporation. (2019b).

CVE Identifiers (also called CVE-ID and CVEs) are unique, common identifiers for publicly known information security vulnerabilities. Each CVE Identifier consist of the following information;

- CVE identifier number
- Indication of candidate status or/and entry
- Summary description of the security vulnerability or exposure
- All essential references (i.e., vulnerability reports or OVAL-ID (MITRE Corporation, 2019b)

The National Vulnerability Database (NVD) is the US government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables e.g., 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; MITRE Corporation, 2019b).

Both CVE and NVD are sponsored by Network Security Deployment National Cybersecurity and Communications Integration Center in the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Division at the U.S. Department of Homeland Security, and both are available to the public and free to use (MITRE Corporation, 2019a; MITRE Corporation, 2019b).

5.5.2 Digital Forensics XML

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

According to Garfinkel (2019), 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 (e.g., the program name, where the program was compiled and linked libraries)
- The state of the computer on which the processing was performed (e.g., 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 cyber-attacks, but also identifying, tracing and prosecuting a criminal/criminal group. This means even multifunctional integration where existing intrusion detection/prevention systems complementing new solutions in the future.

There are no essential barriers to increase collaboration in organizational, tactical, strategical and technical level 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 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 to exchange critical between EU member countries. That means Cyber risks have become common challenges. Havaro 2.0 will improve early detection and preventive functions. Operative public safety functions require quick response or even prediction. HAVARO 2.0 should utilize artificial intelligence (AI) 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 enables to exploit difference databases and produce characterized data more effectively than a human can and it may come to a conclusion by learning from input information. In addition to this, AI can make a decision without human interaction. This means also that not every ECHO participants have the same potentiality or opportunities to develop national system architecture.

International Cyber-physical dimension of threats set requirements, what should be minimum cyber-security 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 3 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.

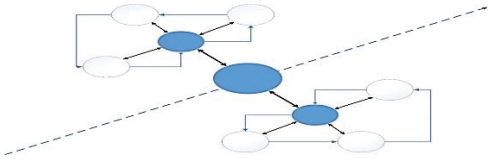

Figure 3: *Connection between sub-hubs*

Therefore ISAC based national sectorial classification is the optimal way to share classified information as Figure 4 illustrates.

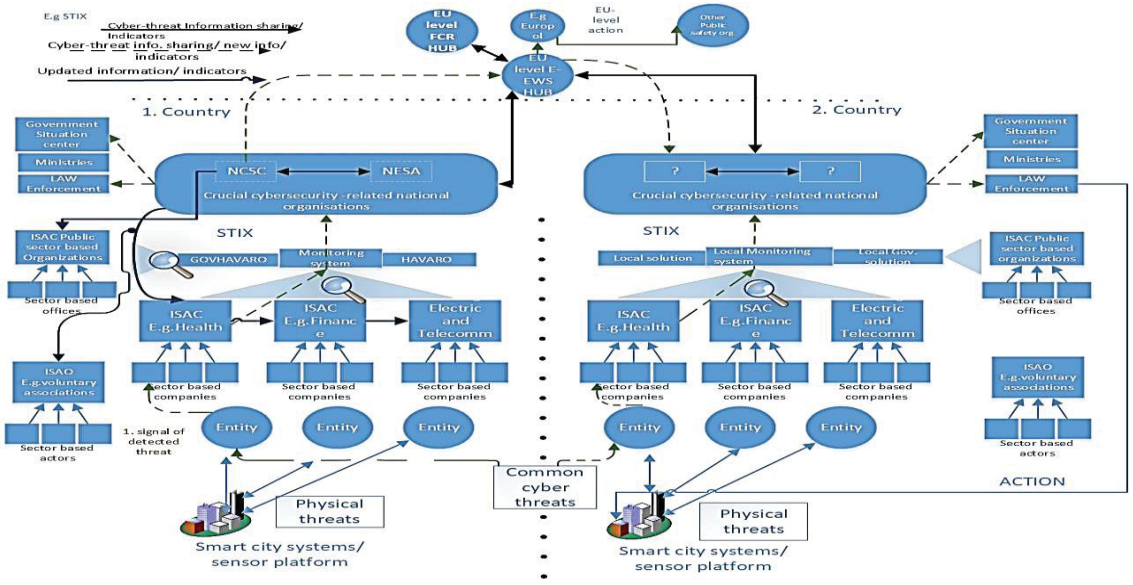

Figure 4: Proposed E-EWS information sharing model

The figure 4. demonstrates information sharing relationships and organizational structure concerning information sharing within a centralized hub system (countries, companies, public safety organizations and other actors). In Country number 1. (Finland) Identifiers of national HAVARO Early Warning System detects a weak signal of cyber-threat concerning internet traffic in a multinational enterprise. The national cybersecurity center of country 2 has not noticed a cyber-threat activity. Automated Information Sharing –functionalities produce crucial data for the central EWS hub, which shares relevant information in near real-time to the situation centers (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 cyber-threat. NCSC of Finland uses a parallel subsystem for public organizations; HAVARO consists of separate early warnings solution named "GovHavaro" for all public organizations.

Participants do not need to share information directly with each other, but there is a need to establish e.g., sector-specific communities called e.g., 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 centers 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. From national systems' point of view, such as the Finnish HAVARO system, centralized EWS hub and sub-hubs is the simplest option. On the other hand, a big challenge will be who maintains the central hub, and what its governance model would be.

References

Apuzzo Matt, (2019). Europe Built a System to Fight Russian Meddling. It's Struggling. The New York Times. Retrieved 11/2019.

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.

Endsley, M. R. (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 2017. Greece: ENISA.
ENISA & ITE. (2017). Information sharing and analysis centres (ISACs) cooperative models. Greece: European Union Agency for Network and Information Security.
EUROPEAN COMMISSION, (2019). Horizon 2020 - Work Programme 2018-2020. 14. Secure societies - Protecting freedom and security of Europe and its Citizens. (2019)4575. European Commission.
EUROPEAN COMMISSION, (2016). EU-U.S. Privacy Shield: stronger protection for transatlantic data flows. Brussels:
EUROPOL. (2019). Secure information exchange network application (SIENA). Retrieved 7/2019, 2019, from 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, 8, 161-174.
GitHub. (2019). Support your workflow with lightweight tools and features. Retrieved 7/2019, 2019, from https://github.com/MISP/MISP-Taxii-Server
Hernandez-Ardieta, J.L.,Tapiador, J.E. and Suarez-Tangil, G., (2013). Information sharing models to cooperative cyber defence. The 5th IEEE International Conference on Cyber Conflict (CyCon) 2013, pp. 1-28
KPMG. (2013). IDS:N käyttöönotto herättää todellisuuteen., 7/2019, from 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. Helsinki: SAINT Consortium/ Traficom.
Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa No. 28. Helsinki: Valtioneuvoston kanslia.
MITRE. (2018). Trusted automated eXchange of indicator information — TAXII™ enabling cyber threat information exchange
MITRE Corporation. (2019a). Common vulnerabilities and exposures. https://cve.mitre.org/cve/cna.html
MITRE Corporation. (2019b). CVE-details. 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, 17(3), 131-148.
NCSC-FI. (2017). Viestintäviraston kyberturvallisuuskeskuksen palvelut. Cybersecurity services of the NCSC-FI. Helsinki: TRAFICOM.
NCSC-FI. (2019). Havaro service and FAQ. Retrieved 7/2019, 2019, from https://www.kyberturvallisuuskeskus.fi/en/havaro-service
NIST. (2019). “National Vulnerability Database - General Information”. [Online]. Available: https://nvd.nist.gov/general. [Accessed 1 9 2019]
Nunamaker, J., Minder Chen, J. R., & Purdin, T. (1991). Systems development in information systems research. (3), 89-106.
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.
OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C). (2017b). TAXII™ version 2.0. Committee specification 01 No. taxii-v2.0-cs01) OASIS Open.
Secretariat of the Security Committee. (2013). Finland´s cyber security strategy - government resolution Ministry of Defense.
Simola, J., & Rajamäki, J. (2017). Hybrid Emergency Response Model: Improving Cyber Situational Awareness. 16th. European Conference on Cyber Warfare and Security, University, College, Dublin, Ireland. pp. 442-451.
TED. (2019). Prior information notice HAVARO 2.0. Retrieved 7/2019 https://ted.europa.eu/udl?uri=TED:NOTICE:453281-2017:TEXT:EN:HTML&tabId=0
The Department of Homeland Security (DHS). (2019). Automated indicator sharing (AIS). Retrieved 6/1, 2019, from https://www.us-cert.gov/ais
White House. (2013a). Critical Infrastructure Security and Resilience, Presidential Policy Directive U.S.C.
White House. 2013b). Federal Register - Improving Critical Infrastructure Cybersecurity, Part III - Executive Order 1363. Vol.77.U.S.C.
Yin, R. K. (2014). Case study research, design and methods (5th ed.). Thousand Oaks: Sage Publications.

Professor Paul W. Poteete teaches information systems and cybersecurity programs at Geneva College. Previously, Professor Poteete worked in New Zealand, the United Arab Emirates, Hawaii, and California in executive leadership roles in industry and faculty roles at several schools. He graduated from the United States Naval Postgraduate School while providing research and joint operations support.

Dr. Dorothy Potter has over 20 years of experience as a Federal Financial Manager. As a Professor of Practice, she currently teaches for the National Defense University College of Information and Cyberspace and is Lead Faculty for the Risk Management, Internal Controls, and Auditing for Leaders graduate course, and provides teaching support to other faculty.

Dr. Paresh Rathod has worked more than 18 years in the fields of ICT and international businesses. Currently, Dr. Rathod is working as a senior lecturer at Laurea UAS, Finland. He is also serving as a Chairman of European Cybersecurity Organisation (ECSO), Brussels. He is actively working in the European and International Research, Development & Innovation (RDI) and business projects.

Dr. Aunshul Rege is an Associate Professor with the Department of Criminal Justice at Temple University. Her cybercrime/security research on adversarial decision-making and adaptation, organizational and operational dynamics, and proactive cybersecurity is funded by several National Science Foundation grants.

David M. Rohret is the lead Research and Development scientist for GDIT's full spectrum cyber red team. He received his Master's in Computer Science from LaSalle University in 1994. He has presented and published in over 25 technical conferences and journals. His current areas of research are autonomous offensive AI systems and alternate coupling effects.

Dr. Joseph H. Schafer is Professor and Chair of Leadership and Strategy, College of Information and Cyberspace, NDU, USA. Joseph has BS in EE & CS from West Point, MS and PhD in CS from GWU, MA in Strategy from Naval War College, and MBA from UVA Darden. His current research focuses on the security implications of influence and strategically disruptive emerging technologies.

Dr. D. Cragin Shelton, CISSP, has experience in supply chain risk management, electronic health system security, insider threat monitoring, identity management, PKI, and network boundary protection. His degrees are in cybersecurity, information systems management, and chemistry. He is a Senior Member of IEEE and ISSA, and a member the Computer Society, (ISC)2, and INCOSE.

Jantje Silomon is a researcher at the Institute for Peace Research and Security Policy in Hamburg (IFSH), having joined as part of the Arms Control and Emerging Technologies Research Project in 2019. Previously, she conducted her doctoral research on the topic of software as a weapon at the University of Oxford.

Jussi Simola works as a DSS specialist in Laurea University of Applied Sciences and he is a PhD student of cyber security in University of Jyväskylä. His area of expertise includes decision support technologies, SA systems, information security and continuity management. His current research is focused on effects of cyber domain as part of Hybrid Emergency Response Model.

Risto Vaarandi received his PhD degree from Tallinn University of Technology (Estonia) in 2005. In 1998-2018, he was affiliated with SEB Estonia and NATO CCDCOE, and since 2015, he is working as a senior researcher in Tallinn University of Technology. His research interests include event correlation, event log mining and analysis, and security monitoring technologies.

Petri Vähäkainu is a project researcher (MSc., BSc.) in Faculty of Information Technology at the University of Jyväskylä in Finland. He has been researching utilization of Artificial Intelligence in Cyber Security, health care and Structural Health Monitoring.

Dr. Cihan Varol is an Associate Professor of Computer Science at Sam Houston State University. He received his Ph.D. in Applied Computing from University of Arkansas at Little Rock in 2009. His research interests are in the general area of information (data) quality and its applications on Digital Forensics and Information Security areas.

Ion A. Iftimie is an Eisenhower Fellow at the NATO Defense College in Rome. Formerly, he served as a Senior Cyber Planner at the United States Cyber Command. He is a graduate of the Harvard Kennedy School Executive Program in Cybersecurity Policies and of the Swedish Defense University Senior Course on Security Policy.

Abdul Bashiru Jibril is a PhD Candidate at the Faculty of Management and Economics, Tomas Bata University in Zlin, Czech Republic. He received his MSc. in Management and Marketing from the same University in 2018. He is a senior research assistant and a team leader of a Faculty-wide project. His main research areas are internet marketing, consumer behavior, and brand management.

Mr. Abiud Jimenez is a principal electrical engineer at Dynetics, Inc. He received his Master in Systems Engineering from SMU in 2006 and his BSEE from UTRGV. His main research involves studying effects on wireless communications systems caused by intended and unintended interference from electromagnetic waves.

Dr Keith Joiner joined the Air Force in 1985 and became an aeronautical engineer, project manager and teacher over a 30 year career before joining the UNSW in 2015 as a senior lecturer in test and evaluation. His expertise includes Defence Test and Evaluation of complex systems and platforms, their acquisition, design acceptance and operational acceptance, including to varying extents land, maritime, aerospace and joint systems and platforms.

Jennyphar Kahimise is a Master of Computer Science student at the Namibia University of Science and Technology (NUST). Her research interests includes Human Computer Interaction, Children safety online and cybersecurity.

Omer Faruk Keskin is a Ph.D. Student in Engineering Management and a Graduate Assistant in Old Dominion University. He holds an MS Degree in engineering management and a BS degree in systems engineering. His research is focused on risk and reliability analysis of critical infrastructure cyber physical systems.

Minchul Kim is a researcher of Agency for Defense Development, South Korea. He is currently in an integrated PhD program in Korea University. His main research areas are integrated cyber situational awareness system and algorithmic optimization.

Mr. Neal Kushwaha is the founder and CEO of IMPENDO Inc, a cyber security and data centre consulting firm in Canada. Annually, he hosts a conference in Ottawa, Canada called DCAR. During his spare time, he climbs big mountains in the Himalayas. Neal is also a recipient of the Silver Medal of Bravery.

Dr Michael Adu Kwarteng is an Assistant professor of Marketing and Management at Tomas Bata University in Zlin, Czech Republic. He received his PhD in Marketing from Tomas Bata University in 2018. His research interest is primarily centred on the application of internet in marketing and currently researching on online buying behaviour of customers in both developed and developing economies

Maxime Lagrasse is a French student from the Bordeaux Institute of Technology (Bordeaux-INP) working towards a five-year engineering degree, in the form of a special curriculum, with half-time lecture attendance and half-time work in a company as a system and network administrator.

Mr. Hyong Lee is a Senior Policy Analyst with NDU's Center for Applied Strategic Learning. His career includes being a Presidential Management Intern with the Army Cost and Economic Analysis Center and Chief, Decision Support Branch at US Pacific Command. He joined NDU in 2002 and provides gaming support to the College of Information and Cyberspace.

Dr. Martti Lehto, (Military Sciences), Col (GS) (ret.) works as a Professor (Cyber security) in the University of Jyväskylä. He has over 40 years' experience in C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical director of the Security and Strategic Analysis MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has over 140 publications on the areas of C4ISR systems, cyber security and defence, information warfare, artificial intelligence, air power and defence policy.