Information Sharing and Analysis Centres (ISACs)

Cooperative models

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

This study was contacted under contract with NASK Poland.

Special thanks to the NCSS experts group (https://resilience.enisa.europa.eu/enisas-ncss-project), We would like to acknowledge all the representatives from the Member States for their contribution to this study and especially:

- **Felix Antonio Barrio Juárez,** Spanish National Cybersecurity Institute (INCIBE), ES
- **Raul Riesco Granadino,** Spanish National Cybersecurity Institute (INCIBE), ES
- **Aurélio Blanquet,** EDP Distribuição, PT
- **Nuno Medeiros,** EDP Distribuição, PT
- **Laurent Weber,** GovCERT, LU
- **Mateusz Górnisiewicz,** Banking Cybersecurity Centre (BCC), Polish Bank Association, PL
- **Johan Rambi,** Alliander N.V, NL
- **Teresa Walsh**, Financial Services - Information Sharing and Analysis Center (FS ISAC), UK
- **Nicolas Reichert,** Airbus
- **Gunnar A. Johansen,** HealthCERT, NO
- **Håkon Grimstad,** HealthCERT, NO
- **Tomas Beinaravicius** Swedbank, LT
- **Hans Oude Alink,** National Cyber Security Center (NCSC), NL
- **G.J.P Peeters,** National Cyber Security Center (NCSC), NL
- **Michael Samson**, Dutch Payments Association, NL
- **Phedra Clouner**, Centre of Cyber Security (CCB), BE
- **Zuzana Halásová,** Cyber Security Department, SK
- **Peter Grebáč,** NSA Liaison Officer of Slovak Republic, BE
- **Bruce Nikkel,** European FI-ISAC

ISBN 978-92-9204-239-4, DOI 10.2824/549292

Table of Contents

Executive Summary

Collaboration is a common objective of every European national cyber security strategy. Collaboration to enhance cyber security at all different levels i.e. information on threats sharing, awareness raising can be achieved in two formal structures: The Information Sharing and Analysis Centers (ISAC) and Public Private Partnerships (PPP). This year ENISA has conducted a study on **Cooperative Models for Public Private Partnership (PPPs) and Information Sharing and Analysis Centers (ISACs)**, collating information on best practices and common approaches.

This study focuses on ISACs. The main objectives of this study are:

- To **provide information about the ISACs in Europe** through collecting information on the current status of ISACs and to identify main models of this type of collaboration.
- To **identify current challenges** that both **the private and the public sector face** in the process of setting up and developing ISACs.
- To **formulate and propose recommendations** to enhance the sophistication of ISACs in Europe.
- To investigate the potential role of ENISA in the creation of Pan European ISAC

Information Sharing and Analysis Centers are trusted entities to foster information sharing and good practices about physical and cyber threats and mitigation. In this report the most common approaches are categorized in three different models: the country focused, the sector specific and the international structures.

The different reasons for creating an ISAC are also presented: the ISAC could support the implementation of new European legislation (e.g. NIS Directive) or support economic interests. In a similar context depending on the rational, the driving forces leading to the creation of the ISAC differ; in some cases, the private sector takes the lead, in others the public sector should bring all stakeholders together.

European ISACs are concentrated on building **partnerships** and **trust** between members. They are largely industry-driven, but governmental support is expected – not in terms of funding, but rather in facilitating functions (secretariat) and offering professional knowledge (fighting cybercrime, sharing information relevant for the industry). Participation of governmental bodies gives the ISAC an increased formality and also corroborates the public sector's respect of industry needs and supports it in facing new challenges (e.g. NIS Directive and GDPR implementation).

The following recommendations have been identified to put forward the role of ISACs:

- ISAC participants should invest in creating trust to ensure right level of information sharing
- ISAC facilitators should ensure right level of engagement by all ISAC participants
- ISAC should have a structure that motivates the private sector to participate
- TLP is a good starting point for information sharing
- ISAC should have a structure that engages the public sector as well (finding balance)
- All member should agree to terms of reference and a code of conduct
- Every ISAC should produce results periodically
- Specific circumstances when mandatory information sharing is required should be agreed
- ISAC should ensure funding mechanisms from the very beginning
- The ISAC should invent on cross sector ISAC collaboration
- Law enforcement could have a specific role in the ISAC
- Evaluation should be performed periodically
- ISAC should develop new services based on their member's needs

1. Introduction

Information Sharing and Analysis Centres (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector. ISACs have created communities within the private sector. They could be oriented on a specific critical sector (e.g. finance, energy, health) or serve as a focal point on the national level to gather information about cyber incidents and analyse it.

ISACs were originally created in the USA. In 1997, after the first terrorist attacks on World Trade Center (1993) and Oklahoma City (1995), President Clinton appointed the President's Commission on Critical Infrastructure Protection (PCCIP). Its objective was to identify the possibility of cooperation between public and private sector so that the US critical infrastructure could be properly protected. Chaired by Robert T. Marsh, the Commission presented the so called "Marsh report" with many recommendations about raising the level of critical infrastructure in the US. One of the main recommendations was to establish Information Sharing and Analysis Centres (ISACs), so as to build and strengthen cooperation between public administration and the industry.

Nowadays, 23 sector-based ISACs make up the National Council of ISACs (NCI) in the USA. Formed in 2003, NCI collect and analyse cyber and physical threat intelligence, sharing this vital information with member companies in their particular sectors. ISACs have the cooperation of the public sector – Department of Homeland Security, where CERT US is located. Some of them are also active in Europe (e.g. FS – ISAC).

Analysis of twenty years of US experience indicates that ISACs are effective and can scientifically enhance the level of cyber security. They create an ecosystem in which trust is being built among critical operators and experience can be shared. Because of this, entities less advanced in the field of cybersecurity could learn from others. Due to the fact that ISACs also cooperate with the public sector, they help increase the overall level of cybersecurity on national level and in the specific sector (for example by cooperating with sectoral authorities).

To ensure the right level of cybersecurity, cooperation between the public and the private sector is absolutely crucial. ISACs create a platform for such cooperation in term of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis. In Europe, the first ISACs focused on the Finance and Energy sector.

Moreover, European legislation nourishes the creation of ISAC: the NIS Directive among others separates the operators of essential services in sectors and tasks the operators to implement requirements on incident reporting. The creation of sectorial ISACs at national level could further assist with the implementation of these provisions. In some countries (e.g. the Netherlands) this kind of structure is already used to build trust among private entities as well as between the private and the public sector. During the transposition of such European legislation to national law, these communities could be further informed and advised by policy makers. Finally, the recently announced Cybersecurity Act suggests the formal creation of European sectorial ISACs supported by ENISA.

1.1 Objective and Scope

This study aims to analyse Europe-based ISACs, to identify common challenges, and to identify best practices. It will result in a clear understanding of the value added and the necessity for future investment in ISACs. It can also be used as a guide to create an ISAC.

For the purpose of this study ISACs has been defined as **member driven organization (comprised by both public and private sector) or group (formal or informal) which is created to support its members in protection by cyber and physical security[1].**

In many EU Member States, ISACs or similar initiatives exist; the research therefore has focused on both formal and informal member-driven organizations or groups that are created with the purpose or objective to support its members in cyber security and related physical security responsibilities.

It is worth mentioning the fact that this study deals with ISACs as a special type of collaboration in the field of cybersecurity. The second type of collaboration is PPPs. The status of PPPs in Europe is covered in another report which constitutes part of the same project: Public Private Partnerships (PPPs) Cooperative models[2]. ISAC are a type of PPP; the main difference is that ISACs are generally more formal than any other types of PPPs in the field of cybersecurity. With each industry sector free to set up their ISAC, the ISAC differ wide in quality, structure and in how they are funded, managed and operated (Prieto, 2006). The whole concept of this kind of cooperation is connected with sharing information and analysis concerning cybersecurity incidents. This reason increases formality in this cooperative model as the actors/stakeholder involved in the process need to follow a clearly defined framework for sharing both information and analysis.

The main objectives of this study are:

- To **provide information about the ISACs in Europe** through collecting information on the current status of ISACs and to identify main models of this type of collaboration;
- To **identify current challenges** that both **the private and the public sector face** in the process of setting up and developing ISACs;
- To **formulate and propose principles** to enhance the sophistication of ISACs in Europe.

1.2 Methodology

To collect data for this study, a qualitative methodological approach was followed with desk research and series of interviews with experts from EU Member States. The desk research was based on publicly available information that built up the questionnaire that supported the interviews. The interviews and consultations covered 17 EU Member States representing stakeholders from the public and the private sector. The validation of the findings was done through a workshop organised in The Hague together with NCSC NL and through the ENISA NCSS experts group.

1.3 Target Audience

The intended target audience consists of the national cyber security authorities, CSIRST community, policy and law makers and in general public and private organisations with an interest in NIS. This report serves as a guide for any stakeholder who would be interested in launching and running an ISAC on cyber security.

1.4 Structure of this document

Chapter 2 explains in a nutshell the driving forces of creation of ISAC and the motivation for the public and the private sector to be part of these initiatives. It also gives an overview of ISAC in the EU. Chapter 3 contains an analysis of common models for ISACs. Chapter 4 presents the governance models for ISACs. Chapter 5 is on information sharing and trust building mechanisms with special focus on their interdependences. It also discusses the role the ISAC have in capacity building. Chapter 6 elaborates on common challenges the ISAC face, and the guiding principles that can take the ISAC a step further. The study concludes with discussion on the evolution of ISAC, ISAC 2.0.

[1] https://www.enisa.europa.eu/publications/cybersecurity-information-sharing
[2] https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/

1.5 EU policy context

DSM Strategy

In May 2015, the Digital Single Market Strategy (European Commission, 2015) was adopted[3]. A number of initiatives are defined by the Commission in this document. Their implementation should open up digital opportunities for people and business, enhancing Europe's position as a world leader in the digital economy.

Because "trust and security stand at the core of the whole DSM strategy" (European Commission, 2015), the Commission leads a number of projects that aim to boost internet trust and security, so that the right environment for digital economy could be created.

In May 2017, the Commission published a mid-term review of the DSM strategy (European Commission, 2017). It took stock of the progress made and called legislators to swiftly act on all proposals already presented, and it outlines further actions on online platforms, data economy and cybersecurity.

The DSM strategy proves that cybersecurity it is not only about homeland or international security. It is also about bolstering the economy among Member States and in Europe as a whole. With the right level of resilience in cyberspace, new types of digital services can develop (e.g. electronic banking), and free provision and supply of services across European borders can be secured.

In the context of the DSM strategy, creating the ISACs' ecosystem in Europe (not only in Members States but also on the European level) could constitute a method of increasing the overall cybersecurity level in the EU and securing the digital economy. At the same time, it could create capabilities for the digital single market and digital economy to grow and develop faster.

EU Cybersecurity Strategy

In 2013, the European Commission presented the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (European Commission, 2013)[4]. The document sets out the EU's approach on how to best prevent and respond to cyber disruptions and attacks as well as emphasizes that fundamental rights, democracy and the rule of law need to be protected in the cyberspace. It was the first strategic document on the European level which referred only to cybersecurity.

Achieving cyber resilience is indicated as one of the strategic priorities and actions, which means that effective cooperation between public authorities and the private sector is absolutely crucial. The strategy also stresses that the national NIS competent authorities should collaborate and exchange information with other regulatory bodies.

From this perspective, ISACs could be useful as platforms of effective private – private, public – public and private – public cooperation in the field of information sharing. This kind of collaboration allows increasing the overall level of security in Europe.

NIS Directive

The NIS[5] Directive (EU) 2016/1148 was adopted in July 2016[6]. The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It imposes on the Member States the obligation to establish Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192
[4] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
[5] Network and Information Security Directive
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

The scope of the Directive covers two kinds of entities: operators of essential services and digital service providers. Both the essential service operators and digital service providers are required to notify incidents. What is also required of them is taking appropriate and proportionate technical and organisational measures to manage risks posed to the security of network and information systems which they use in their operations.

The NIS Directive also creates a mechanism of cooperation among all Member States. There are two mechanisms to do it: The Cooperation Group and the CSIRT Network.

The implementation of the Directive could be a huge challenge for Member States, especially when identifying operators of essential services. It should be decided how it would correspond with the already identified operators of critical infrastructures. It should also be decided what types of incidents will be reported.

Sectoral ISACs can support the smooth implementation of the NIS Directive by being the placeholders for the interaction between the public and the private sector stakeholders.

Communication on Strengthening Europe's Cyber Resilience System

In July 2016, the European Commission presented the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (European Commission, 2016)[7]. The document contains three goals: stepping up cooperation to enhance preparedness and deal with cyber incidents; addressing challenges facing Europe's cybersecurity Single Market; nurturing industrial capabilities in the field of cybersecurity.

In the field of information sharing and cooperation among Member States, the Commission decided to prepare the cooperation blueprint to handle large-scale cyber incidents on the EU level (which is currently under discussion). Additionally, it decided to facilitate the creation of an 'information hub' to support the exchange of information between EU bodies and Member States, as well as work in close cooperation with Member States, ENISA, EEAS and other relevant EU bodies to establish a cybersecurity training platform. The Commission also pointed out that "At European level, Sectoral Information Sharing and Analysis Centres (ISACs) and corresponding CSIRTs can play a key role in preparing for and responding to cyber incidents. Such ISACs have already been already created. There is the FI-ISAC in the **financial sector**, EE-ISAC in the **energy sector** and ISAC in the **aviation sector** is also being created.

All these sectors have cross-border dependencies and both services and infrastructures in those sectors are shaping throughout the territory of several EU Member States. Thus, creating international, pan-European ISAC could be very useful." (European Commission, 2016). Information exchange between different stakeholders is extremely valuable to secure European cyberspace and enable business and the Digital Market to grow.

[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

Joint Communication on Resilience, Deterrence and Defence

In September 2017, the European Commission presented the joint Communication on resilience, deterrence and defence: Building strong cybersecurity for the EU[8]. This Communication aims at building a strong single market through an EU cybersecurity certification framework, through a blueprint plan for operationalising cybersecurity response through investing in strong encryption and protection of fundamental rights, through strengthening ENISA's role and developing international cooperation for EU leadership on cybersecurity. The Communication recognises ENISA's role in the implementation of the NIS Directive and addresses a stronger role for the Agency through a proposal for a permanent mandate.

"The role of Information Sharing and Analysis Centers is particularly important in creating the necessary trust for sharing information between private and public sector. Some first steps have been taken in respect of specific critical sectors such as aviation, through the creation of the European Center for Cybersecurity in Aviation, and energy, by developing ISAC. The Commission will contribute in full to this approach with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NISD."

[8] http://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PD

2. Formation process

The ISAC' formation process is multi-dimensional. In the beginning, it is about the rationale of creation. There are multiple reasons to create ISAC. These reasons are linked to cultural issues and differ among Member States. In countries with a long-lasting tradition of strong public authority and strong public administration, the most important motivation is usually a regulatory requirement. Whilst in countries with a tradition of sharing power, the approach is more pragmatic and the most common reasons are economic and social interests.

Another problem for creating an ISAC is the dominant driving force; although the cooperation of public administration and industry is essential, in most countries it is the private sector that is the driving force for the creation of ISACs. It is apparent when reasons of cooperation are analysed (see: subchapter 3.3). For the private sector, it is mainly about business profits, which are well addressed by ISAC (e.g. access to knowledge, networking). For the public sector the overall better understanding of the industry and having knowledge about cybersecurity at the state level is a motivation. In detail, European governments prefer the industry to create ISACs and share information with the public administration, mainly because of the lack of resources (both human and financial) to support this kind of cooperation. There are of course countries where the public sector is more involved in the process of formation of ISACs, but in general there is a hesitation. The main reason is the fact that sharing sensitive information with the private sector is (regarded as) complicated for public entities. Consequently, public servants tend to argue that they will not be able to meet private sector's expectations (more about sharing information between public and private entities in chapter 6).

For the purpose of this study, the term ISAC has been defined as **denoting a member driven organization or group (formal or informal) which is created to support its members in protection by cyber and physical security[9].**

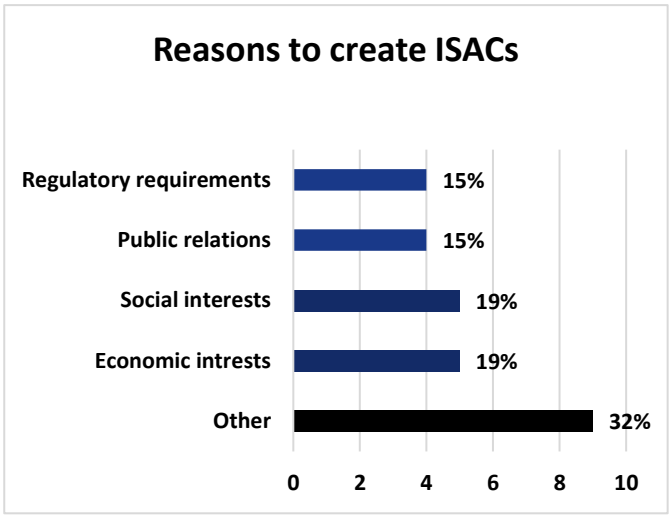
In many EU Member States, ISAC or similar initiatives exist; the research therefore has focused on both formal and informal member-driven organizations or groups that are created with the purpose or objective to support its members in cyber security and related physical security responsibilities.

It is worth mentioning the fact that this study deals with ISACs as a special type of collaboration in the field of cybersecurity. The second type is PPPs. The status PPPs in Europe is covered in another report which constitutes part of the same project: Public Private Partnerships (PPPs) Cooperative models. The main difference is that ISACs are generally more formal than any other types of PPPs in the field of cybersecurity. With each industry sector free to set up their ISAC, the ISAC differ wide in quality, structure and in how they are funded, managed and operated (Prieto, 2006). The whole concept of this kind of cooperation is connected with sharing information and analysis concerning cybersecurity incidents. This reason increases formality in this cooperative model as the actors/stakeholder involved in the process need to follow a clearly defined framework for sharing both information and analysis.

[9] https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

2.1 The rationale

There are multiple reasons to create an ISAC. The chart below depicts the answers of the interviewees and are further described:



- **Regulatory requirements**. ISAC are being created because there is a specific law which obliges the industry to share information (with the public administration) or they are created to support the implementation of the law as an advisory body e.g. European aviation ISAC, European Energy ISAC, Banking Cybersecurity Centre in Poland.
- **Economic interests.** For the private sector this is usually the most common reason to establish ISACs. Usually the growing number of threats and incidents demonstrate that sectorial cooperation is essential to strengthen one's defence. It starts informal and then evolves into a more sophisticated[10] structure of cooperation. Economic interests have two aspects. The first one concerns preventing incidents from happening and having a better overview of the threat landscape e.g. multiple ISACs facilitated by the National Cyber Security Centre in the Netherlands. The second concerns the fact that it is cheaper for an entity to be part of an ISAC and get information from it than to pay for information on the market. Sometimes an ISAC offers also joint services, so that members could have a better price when buying cybersecurity services from IT security companies e.g. CERT.LU is providing services to the members of the group.
- **Social interests**. Beside economic interests, social interests are the second most common reason to establish ISAC. This is mainly the reason for entities with huge experience and know-how in terms of cybersecurity. They tend to have a social interest in sharing knowledge with ones that are not as developed or have fewer resources (money, people) involved in the cybersecurity. Larger companies understand that sharing knowledge within the sector helps them secure their assets better: when a cyber-threat occurs, it is rarely limited to a single enterprise or sector. Collaboration provides them more certainty that their firm is less vulnerable. Social interests are also the rationale of the public sector. Public administration has a responsibility for securing the state as the whole. Because of this, the creation of ISAC in essential sectors, and getting involved in them, offers an opportunity to transfer experience and know-how from one sector to another in order to increase the level of cybersecurity in the country e.g. forum for information exchange in Lithuania, PT CSIRT Network.
- **Public relations**. When an organisation is the critical operator (e.g. banking sector, energy sector), it is important to communicate that the company is safe and will deliver services even if an incident occurs. Therefore, positive public relations could be a reason for the top management to invest in cybersecurity. This puts cybersecurity on the strategic agenda, as it is no longer the interest of the IT or security departments themselves, but of the company as a whole. The same reason applies to decision makers in the public sector. Public relations in terms of good cooperation with the industry put cyber issues on the political agenda and result in creating the national strategy, law and programs, which supports the creation of ISACs e.g. CERT.LU in Luxemburg.

Only one reason is not enough to create an ISAC. Usually, a combination of several reasons is needed - economic and social interests which bring the sector into cooperation and then involve also public entities, which could also accompany by a new law which requires the exchange of information.

[10] Sophistication is used –as change from the natural character or simplicity, or the resulting condition.

Other reasons. There are also other reasons to create ISACs. These are:

- The sector already had some kind of cooperation in place and decided that it should be used to exchange information about incidents e.g. FI-ISAC.NL in the Netherlands,
- Research projects are conducted in critical sectors to provide a good understanding of the needs in the field of security, which on the one hand creates a baseline for cooperation and on the other hand proves that there is a need to create a structure which will support it, gathering security community in one place (realising that the cooperation is a strength and that security should not be an element of competition usually is the result of exchanging information about incidents and threats and sets in motion the entire cooperation process) e.g. European Energy ISAC.

The figure below presents reasons for the creation of ISACs

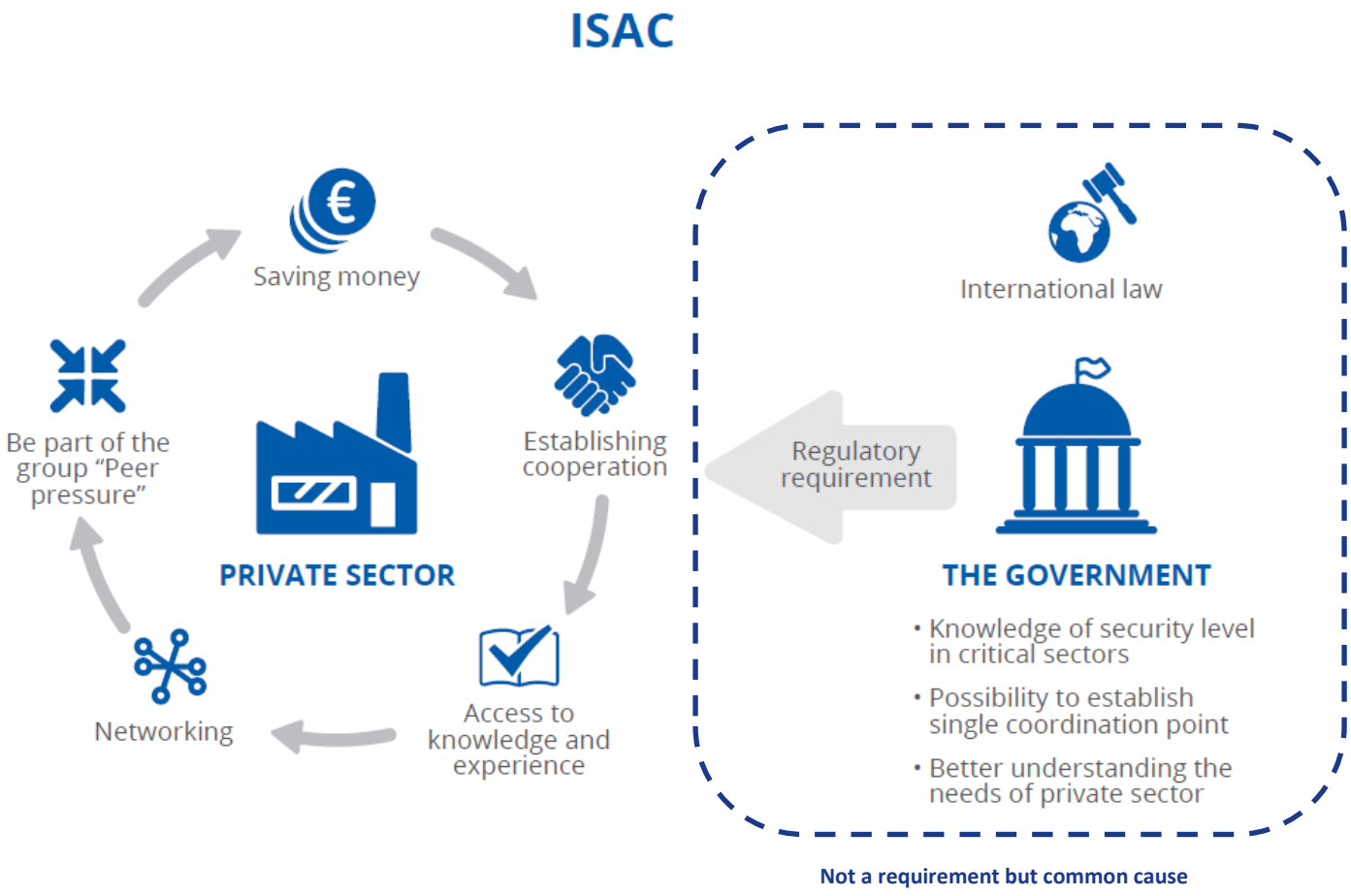


Figure 1: Reasons for the creation of ISACs

2.2 Driving forces for creating an ISAC

Depending on the cybersecurity culture in the country/sector the driving entity for the creation of an ISAC might differ. Mostly the private sector, European institutions or government act as driving forces:

- In most cases it is the **private sector** that initiates the process of setting up ISACs. It is often supported by the government through a facilitator role and through the provision of funding. Usually, when an ISAC is created in one critical sector, the government tries to support others to follow its example and stimulate the growth of ISACs e.g. multiple ISACs facilitated by the National Cyber Security Centre in Netherlands, multiple ISACs facilitated by the National Cyber Security Centre in Finland.
- An interesting example is that there are international ISACs which are supported by **European institutions** (ENISA, Commission) i.e. European aviation ISAC facilitated by EASA and ENISA, European Energy ISAC and ENISA, DENSEK as a European project funded by DG HOME.
- Finally, the initiative to create an ISAC may come from the **government**. In this case there is usually an entire project launched with funding and an action plan e.g. CERT.LU in Luxemburg, multiple ISACs facilitated by the Centre for Security Belgium.

2.3 Motivation

Being part of an ISAC requires to dedicate resources, time and expertise; in the private sector this can be costly so motivation should be strong. Knowledge on cybersecurity together with information on incident response are the most common reasons to participate in an ISAC. The desk research indicated the different aspects of motivation to engage in an ISAC. These are summarised in the Table below:

PRIVATE SECTOR REASONS TO PARTICIPATE IN AN ISAC	PUBLIC SECTOR REASONS TO PARTICIPATE IN AN ISAC
Sharing knowledge about incidents and cybersecurity It helps raise the level of cybersecurity in the organization which is a member of an ISAC and prevent/ respond to the incidents which occur.	**Knowledge of security level in critical sectors** Being a member of an ISAC gives the public sector access to knowledge about the cybersecurity level in critical sectors. It also provides information about threats and incidents. This is helpful as it enables them to better fulfil their legal tasks.
"Be part of the group" "Peer pressure" Entities want to take part in an ISAC because it enables them to confront their ideas and experience with other organizations and learn from the best practices.	**Opportunity to establish a single coordination point** Being a member of an ISAC gives the public sector an opportunity to create a single coordination point, which has been proven to be very beneficial in the case of large-scale incidents. This enables them to better fulfil their legal tasks.
Access to knowledge and experience For an organization which is not so sophisticated in the field of cybersecurity, an ISAC is a fast and efficient way to get all the knowledge and experience which normally takes a lot of time	**Better understanding the needs of private sector** Thanks to close cooperation with the industry, public entities get better understanding of the private sector which has proven useful during setting up of new legislation and cybersecurity strategy. This enables them to better fulfil their legal tasks.
Networking Being a member of an ISAC is a good way of networking and meeting people from different organizations. In the presence of an incident and need to gather information, there is always a know-how way to network with the respective team.	

Figure 2. Private and public sector reasons for participation in ISACs

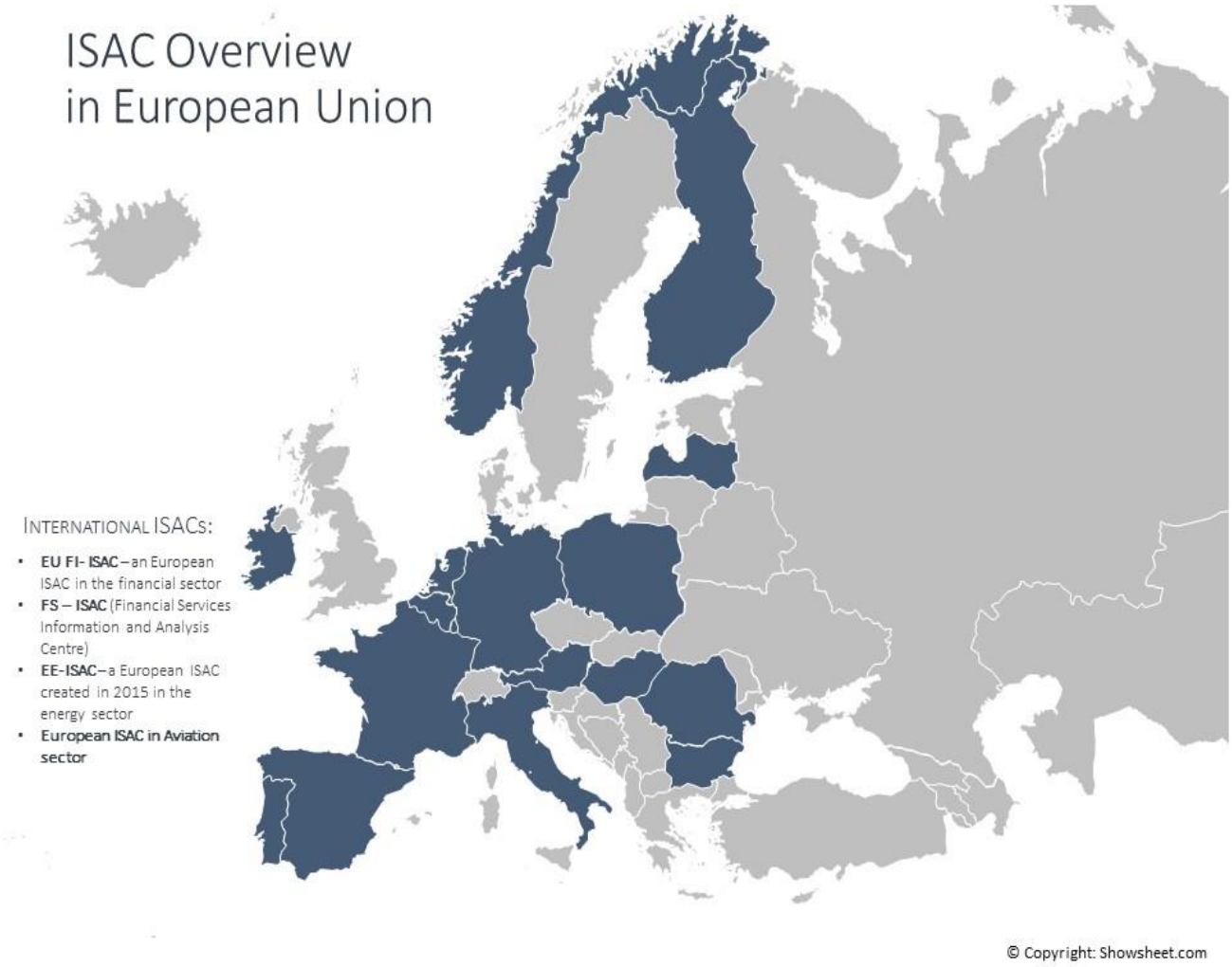
2.4 Overview of ISACs in the MS

European ISACs have different dynamics and specificities than their American counterparts. Firstly, because they were created later and were able to use the knowledge coming from across the Atlantic. Secondly, because European specifics are significantly different than the American. This is linked to the cultural differences – whereas in the US business should take care of itself, in Europe there is an expectation that the state is involved in protecting industry and supports it.

European ISACs are concentrated on building **partnership** and **trust** between members. They are very industry-driven, but there is also a forceful expectation for governmental support – not in terms of funding, but rather of facilitating functions (secretariat) and offering specialist knowledge (fighting cybercrime, sharing information relevant for the industry). Participation of governmental bodies gives the ISAC increased formality, corroborates the public sector's respect of industry needs, and support it in facing new (policy related) challenges (e.g. NIS Directive and GDPR implementation).

The development of the ISACs ecosystem in Europe is dependent on cultural determinants of different member states and the overall level of trust between public and private entities. Because of that, for countries where this trust is not sufficient, it may be suitable to start developing PPPs structures first and then transforming them into ISACs. This is because the exchange of information about incidents, threats and vulnerabilities demands extensive level of trust between entities.

All the above-mentioned findings are derived from interviews with stakeholders and from discussions in the validation workshop. The map below presents an overview of ISACs in Member States. The Annex provides more information.



The common challenges identified were the **lack of trust** between the private sector and public sector and the **lack of a governance model** and clear description of roles that could adhere to the needs of the group. The major issue where the EU still lacks behind is the **analysis** part. Still very few ISAC have built the capacity to support this feature which would scale up in the case of sectoral ISAC. Bright examples of sectoral ISAC are the EE ISAC and the EU FI-ISAC, however all other sectors (like Health, Maritime etc) lag behind on creating ISAC.

3. ISAC models

3.1 Models of ISACs in Europe

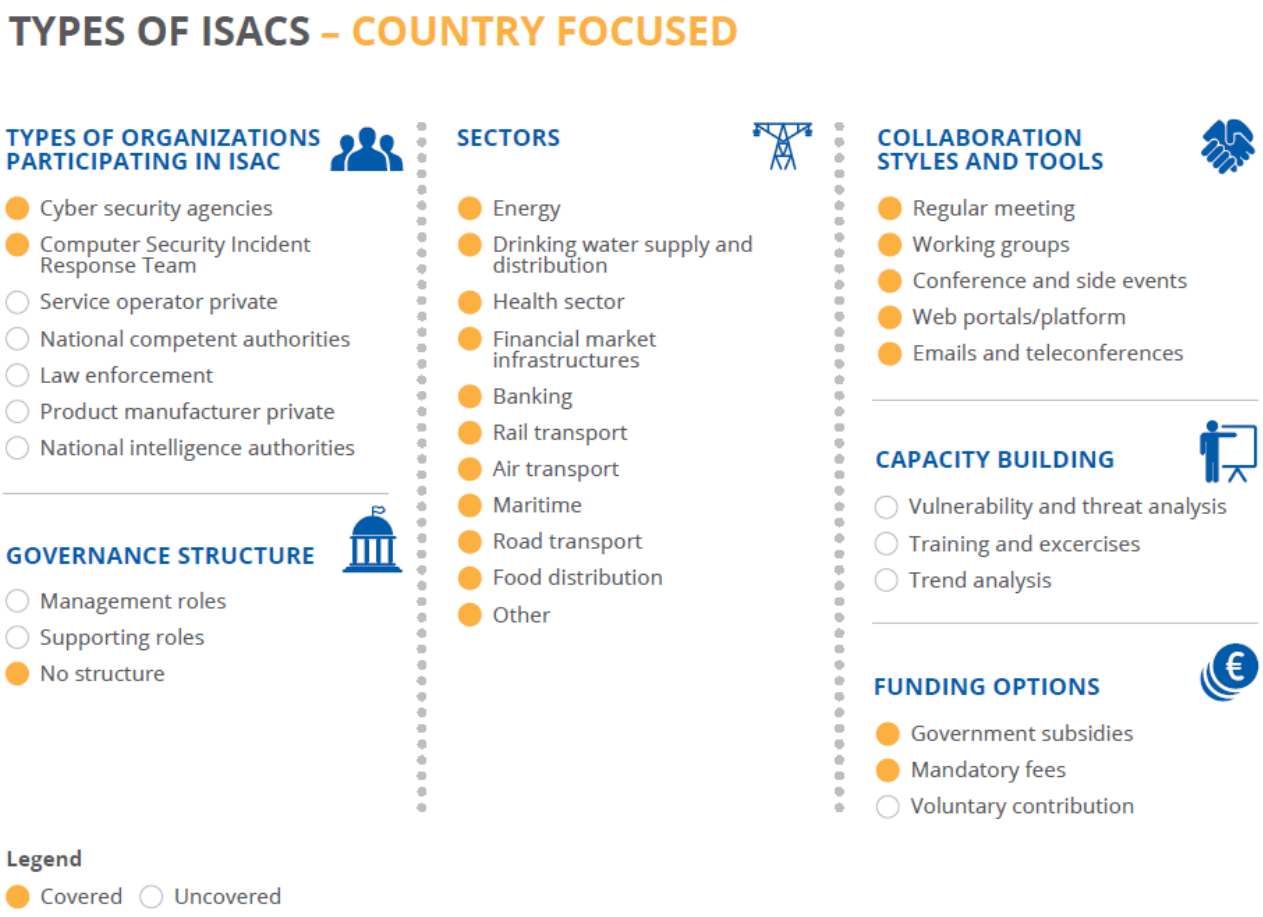
The information collected revealed a common informal categorisation of ISAC models:

- the country-focused model;
- the sector-specific model;
- the international collaboration model.

A brief description of each of them has been given below. At the end of this chapter, a matrix mapping all aspects of each type has been presented.

3.1.1 Country-focused

This type of cooperation and collaboration is focusing on the whole country. The goal is to gather all experts/ CSIRTs under one initiative and make the information sharing, as well as the analysis exchange smoother and more effective. Generally, these types of cooperation are very informal. Most of them are governed by the CSIRTs community itself or experts who participate in the ISAC.



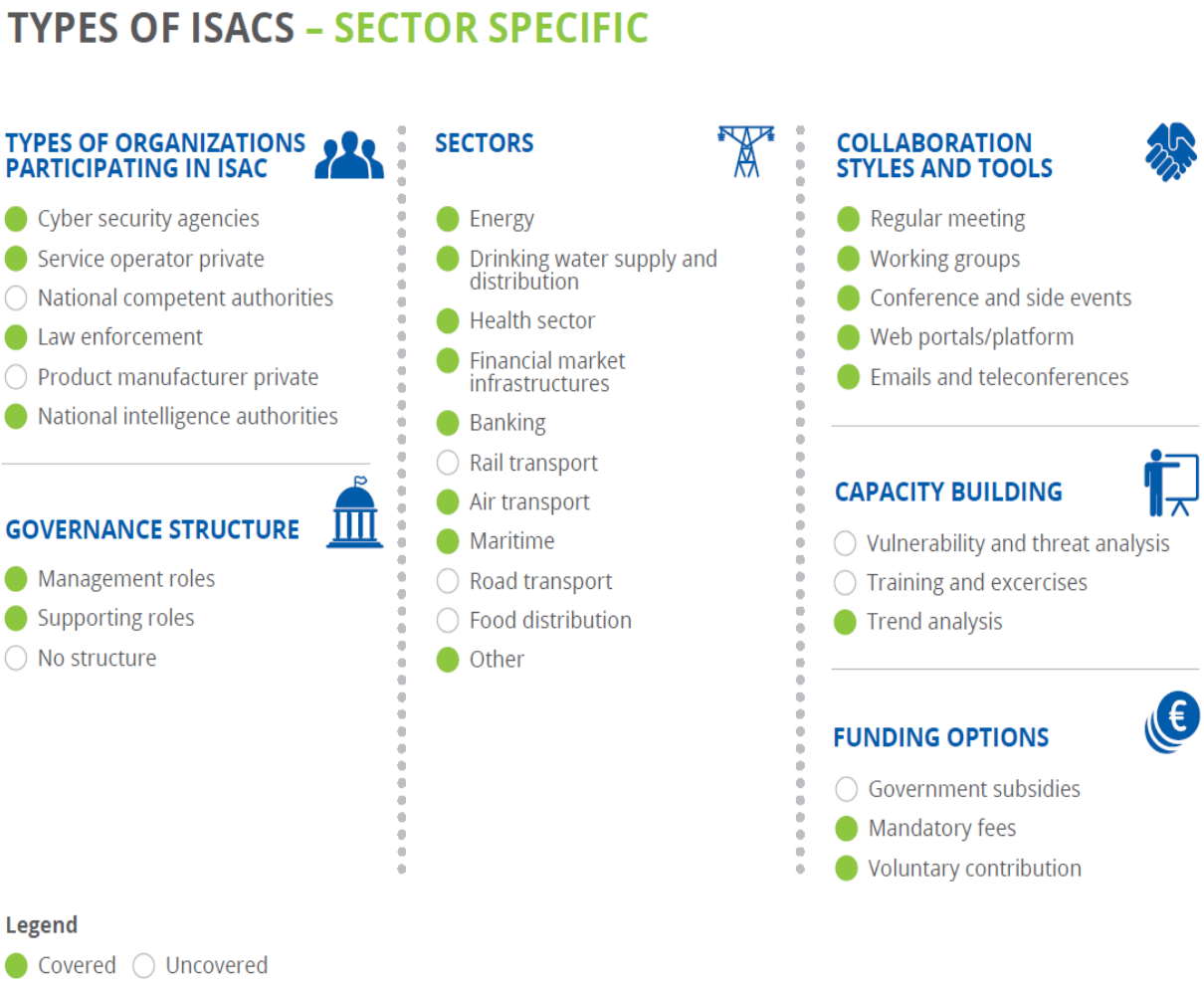
Examples:

- **ICARO (Spain)** – powered by the Spanish National Cybersecurity Institute; based on the Malware Information Sharing Platform[11] example; provides an opportunity to share information among public and private organizations. To join ICARO, the organisation is required to sign a simple agreement.
- **National network of CSIRTs (Portugal)** – initiative of 31 CERTs from Portugal, initiated in 2008, with representatives of both public and private sector's CSIRTs (Government, Energy sector, Financial sector, Telecom sector, Academia, LEA, Intelligence community and Industry). The main objectives of the National Network of CSIRTs are: promoting security culture in Portugal, developing KPI and national information statistics on security incidents for the improvement of proactive and reactive countermeasures, creating the necessary preventive instruments and providing advice in large-scale incident scenarios (between CSIRTs and with law enforcement agencies and intelligence community).
- **Forum for information exchange (Lithuania)** – volunteer community of experts with individual membership, independently on the organisations they represent (if a person changes a job, he or she still remains in the network). The goal is to gather cybersecurity experts in one place for sharing knowledge, expertise and information about threats.
- **CERT.LU (Luxemburg)** – national initiative for all CERTs from Luxemburg, created to exchange expertise and knowledge (network of CSIRTs in the country). CERT.LU is governed by the CERT community itself. Ministry of Economy supports the initiative and all members contribute.

[11] https://www.circl.lu/services/misp-malware-information-sharing-platform/

3.1.2 Sector-specific ISACs

This type of cooperation is focused on the sectorial level of critical infrastructure or essential/vital sector. The goal is to share information and analysis with other information and security experts that are active within the sector, so that the operator could benefit as much as possible from sectorial knowledge and experience. Often enough ISACs are becoming a platform for shared services – members could gain access to security services cheaper as members of a group and negotiate better conditions.



Two different types of cooperation are identified for sector-specific ISACs: ISACs facilitated by the sector itself and ISACs facilitated by the government.

Sector operators facilitated ISACs is a type of cooperation and collaboration where the sector itself decides on the structure of information sharing needed. There is no funding from the government and usually no support from the public sector at all. However, the cooperation with the public sector and public administration exists, for example under specific circumstances like combating cybercrime and exchanging information about incidents (the NIS Directive and its implementation). Generally, this type is more commonly recognised in larger countries which have a strong private sector with well-defined goals in cybersecurity and social interest in sharing its knowledge and experience. When the industry is strong and understands the nature of cyber-threats as well as the need for cooperation, there is usually more budget allocated on ISACs.

Examples:

- **Banking Cybersecurity Centre – BCC (Polish Bank Association), Poland** – a platform for banks to communicate in cases of incidents, as well as to exchange information about vulnerabilities and threats. Beside incidents, BCC provides also other services. To join the BCC banks, the declaration of membership needs to be signed. Every commercial bank can join. At this moment 23 banks (83% percent of polish commercial banking sector) are members of BCC.
- **HealthCERT, Norway** – a joint information security competence centre for the Norwegian health care sector, having of ca. 400 members. The centre shares knowledge about ICT threats and protection mechanisms and continuously monitors traffic within the health IT network. The goal is to prevent and remediate adverse ICT security incidents and malicious intrusion attempts. The government provided funding and resources for the CERT and decided what kind of services it should provide (sensors platform, penetration testing, vulnerabilities assessment and network scanning).

Government facilitated ISACs are generally a joint initiative of both the private and the public sector. The government facilitates the discussion by providing a secretarial role and sometimes provides financial assistance (organising workshops etc.). The characteristic approach in this model is that the public sector tends to have a multi-sectorial approach. This means that ISACs are created not in just one but in many sectors in an attempt to enhance cybersecurity in all sectors. Often, the public administration tries to stimulate ISACs for example by providing some guidance about maturity and delivering best practices from other sectors so that ISACs could interact also with one another and use the experience of other sectors to grow. What was underlined by experts during the interview was the fact that every sector is different. It has a different dynamic and specificity, and also different expertise is involved. Because of this, ISACs specificity differs not only between countries but also between sectors.

Generally, ISACs that are facilitated by the government are characteristic for smaller countries where it is easier for the public sector to facilitate and stimulate it. First and foremost, because there is a smaller number of stakeholders - it is easier to facilitate and stimulate multiple sectors and create a nationwide strategy in this area. This brings us to the second reason: it is easier to secure a budget for initiatives like ISACs in smaller countries.

Examples:

- **Finland** – multiple ISACs are facilitated by the National Cyber Security Centre. NCSC-FI acts as a single point of contact and competence center for cyber security in Finland. NCSC-FI is the Finnish contact point internationally when it comes to cyber security threats and incidents. NCSC-FI gathers, analyses information on security threats from various sources (ISACs, Early Warning and Detection System etc.). Information is then distributed to NCSC-FI's constituents via different channels, including ISACs.
- **Belgium** – multiple ISACs are facilitated by the Centre for Cybersecurity Belgium. The Centre for Cybersecurity Belgium is the main authority for cybersecurity in Belgium. It is currently in the process of creating an Early Warning System to provide critical infrastructure sectors with rapid, standardised alerts about new cyber threats and attacks. A shared platform enables these sectors to access alerts informing them of intrusions and other cyber threats. Because of that, they will be able to be quickly informed by a reliable source and to act without undue delay. The Early Warning System is expected to be up and running by end of 2017. The CCB is issuing e-mail alerts in the meantime.
- **Netherlands** – facilitating the running of the ISAC is a shared responsibility in the Netherlands. The NCSC has the role of the secretariat, thus facilitating the process, but also the industry stakeholders organise the meetings, thus again facilitating the process. It's team work.

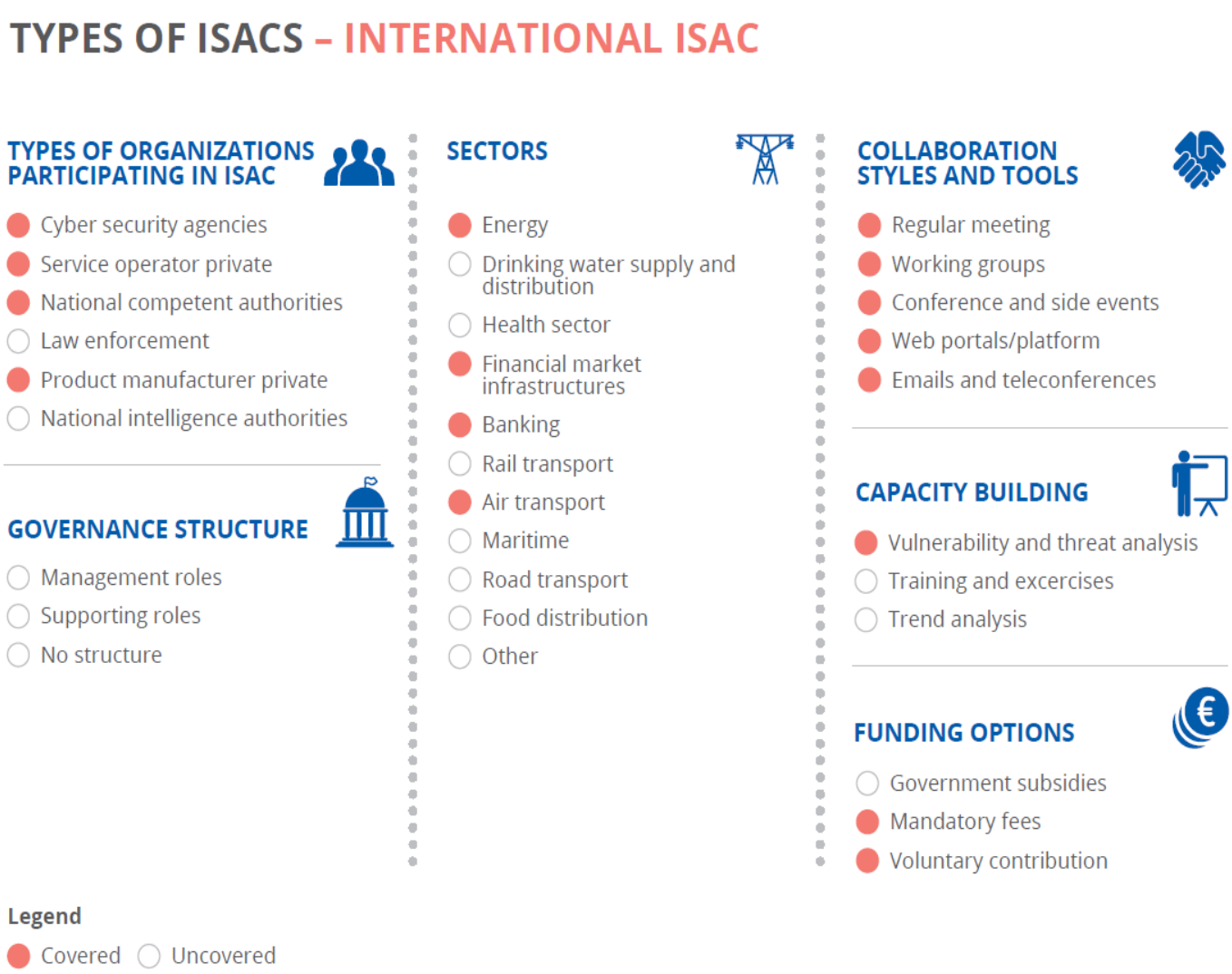
It important to notice that no cross sector information exchange mechanism exists for these kinds of ISACs (energy ISAC to finance ISAC). The mapping of interdependencies between sectors at a national and cross border level will show that this kind of collaboration between cross sector ISAC can bring great results.

3.1.3 International ISACs

These types of ISACs bring together multi-stakeholder members from all over Europe and worldwide. There is a common understanding that cybersecurity is not limited by national borders. Therefore, cooperation is needed. However, some sectors, due to their specificity and cybersecurity maturity, are more willing and eager to participate in this type of ISACs. Sectors which have created or launched an initiative to create ISACs on the European level are: financial/ banking sector, energy sector and aviation sector.

For this type of ISAC, the private sector is the driving force in both the creation and then development, and stimulation. The secretarial function is usually provided by one of members when others take care of marketing, strategy, or recruiting new members. This joint responsibility keeps all stakeholders active. On the other hand, members have noticed that there are no dedicated resources focusing on the ISAC activities, impeding the ISAC's growth.

The main challenge for this case is the fact that the process of building trust is more difficult than in the case of country-focus and sector-specific ISACs. The main reason is the cultural differences – stakeholders from different states have distinct perspective and approach to information sharing.



Examples:

- **EU FI- ISAC** – a European ISAC that serves the financial sector, established in 2008 as the PPP – an initiative of a board member from ENISA; it is a self-supporting group with a chair and a secretary which meets twice a year[12]. Members group consists of country representatives coming from the financial sector, national and governmental CERTs as well as Law Enforcement Agencies (LEA's). Other organisations represented are: ENISA, Europol, the European Central Bank (ECB), the European Payments Council (EPC) and the European Commission. The European FI-ISAC is actively supported by ENISA. The mission of the European FI-ISAC is information exchange on e- and m-channel, cards, central systems and all ICT related topics including: cybercriminal activity affecting the financial community, vulnerabilities, technology trends and threats. Such information exchange helps each member and the banks in their member states to raise awareness on potentials risks, and provides early

[12] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership

warnings on new threats and MO's. It is a self-supporting group with a chair and a secretary; the group meets twice a year[13].

- **EE-ISAC** – a European ISAC created in 2015 that serves the energy sector. It is composed of 22 members (different organisations: utilities, vendors, academia and other stakeholders active in the energy sector). This ISAC was initially created under an EU funded project DENSEK. EE-ISAC Members are sharing: real-time security data and analysis, reports on security incidents and cyber breaches, technical and operational experiences with applied security solutions, lessons learned from past security issues, future challenges and security outlooks and warnings[14].
- **European ISAC in Aviation sector** – an ISAC under creation, initiated in February 2017 by the private sector in cooperation with ENISA and EASA[15]. ECCSA will contribute to the safety of air travellers and the public by assisting in the establishment of acceptable levels of protection of its infrastructures: from design to decommissioning of aircraft; Communication, Navigation and Surveillance systems; and other critical services necessary to the safety of flight.

[13] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/finance/european-fi-isac-a-public-private-partnership
[14] http://www.ee-isac.eu/about
[15] https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-cooperate-cert-eu-cybersecurity

3.2 Actors

ISACs involve stakeholders from both the private and the public sector (56% - 44% ratio) based on the experts interviewed and the ISAC studied. Although the reason for establishing ISACs is to enhance the information and analysis sharing, types of commitment and involvement in such initiatives differ according to the type of organization. It is apparent that there are different reasons and different types of activities among ISACs for public administration and the industry. Moreover, the law enforcement agencies and intelligence community also have different roles to play. Some ISACs involve academia, but the rules of their involvement are quite unique in comparison with other actors.

At this point it is important to notice that multinational or large cyber security companies (European or not) do not tend to participate in ISACs. This is mainly due to the lack of trust ISAC members have towards these companies based on the believe that these companies might use the information and knowledge shared for their own business interests or developments. The benefits of such a participation would need to be investigated.

Three different roles are distinguished in 'the ISAC': the facilitator, the member and the partner. The facilitator is the one setting the logistics of the group (secretarial role); the member is the organisation actively sharing and receiving information and/or paying the membership fee; the partner is the entity that can participate in dedicated sessions usually to offer specific information (scientific data) or to discuss a specific topic (transposition of a Directive to national law).

In this subchapter, information about the activity of each type of stakeholder will be provided. Types of organisation participating in ISACs are presented and below (based on the input from interviews):

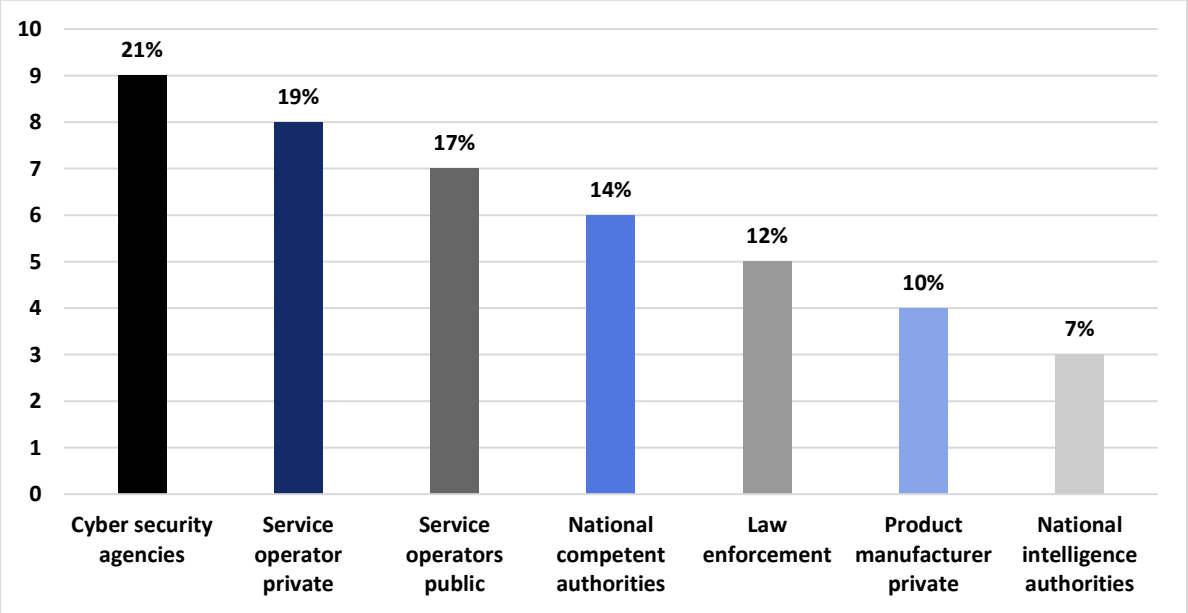


Figure 3 Types of organisations participating in ISAC

3.2.1 The role of public administration

Public administration tends to have two main roles in ISACs. The first one is supporting the industry or potential ISAC members through facilitation of ISACs – providing places to meet and secretarial functions. Sometimes government also allocates funding to set up and further develop ISACs. The second role is connected with creating a legal framework for both the exchange of information and creating ISACs. Legal framework refers not only to legal

regulations, but also to government programs and national cybersecurity strategies. Overall the public administration is a facilitator.

The role of public administration also varies according to their task. National Cyber Security Agencies (NSA) are types of organizations that are involved in almost every ISAC. In some cases, the competent authority might have a secretarial role (e.g. NCSC in NL, NCSC in PT) or might actively participate in the information exchange and analysis (e.g. CCB, NCSC in NL). Most NSAs operate a national or a governmental CSIRT, which is also the focal point for incident reporting and handling for critical sectors. Even if NSAs are not involved directly, they are linked to the ISACs in some way and collaborate with them. However, since NSAs are tasked by governments to ensure a high level of cybersecurity in Member States, their involvement in and support for ISACs is common. It must be highlighted at this point that 1-2 public bodies participate in ISAC and usually in dedicated sessions; the graph above explains the common types of public bodies that are present in these sessions.

Usually different rules of participation in ISACs apply to public administration than apply to the industry. On the operational level, because of the sensitivity of information they could share (for example classified information), on the management level, because the government tends to let the industry perform managerial roles. However public and private parties in an ISAC should obey to the same rules; this is often a great challenge as if not, there is no reciprocity in the co-operation.

It should be noted that sectoral regulators are seldom part of ISACs This is because the information exchange process could be compromised when entities which could impose sanctions on private sector are part of the forum for exchange of information about vulnerabilities.

3.2.2 The role of industry and critical infrastructure operators

The industry is the main driving force of all ISACs. Firstly, because ensuring high level of security and continuity of its businesses is the main interest for the private sector. As the sector depends increasingly on IT technologies and their smooth functioning, cyber aspects are increasingly crucial for the industry's security. Secondly, the industry is obliged by law to report incidents and to ensure continuity of critical services (e.g. critical infrastructure and crisis management regulations). Finally, because he private sector is the asset owner of the majority of the infrastructures.

Therefore, in most of the cases the industry chairs and governs ISACs all over Europe. Even when public administration is involved, it is the industry that determines the shape and functioning of their cooperation. The level of information sharing and collaboration always depends on the level of involvement and dedication of the industry representatives. The industry is therefore either a facilitator or a member in the ISAC. In case a representative from another sector participates sporadically in the ISAC meetings (probably dedicated open session), they become partners.

The chart below presents the industry's involvement in ISACs, broken down by sectors.

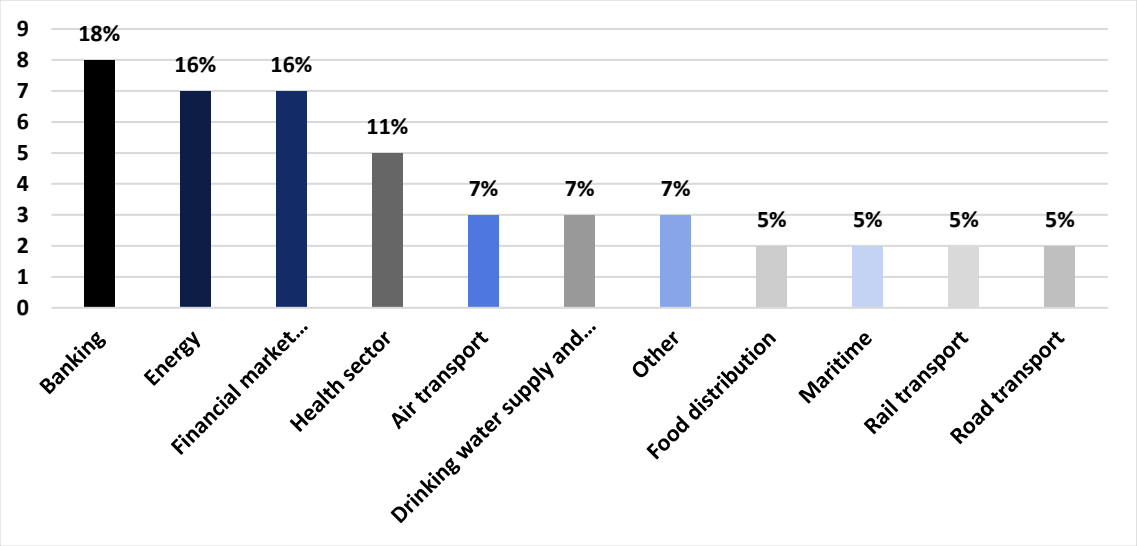


Figure 4 Sectors involved in ISAC

Two sectors in particular are more developed in this sphere than others: the financial sector and the energy sector.

Because of its nature, the **financial sector** is highly exposed to cyber-threats and cyber-crime. A successful attack on the financial infrastructure gives the criminals access to money and results in loss of trust, not only for a single bank but for the whole sector and services it delivers (e.g. electronic payments). So financial companies see cybersecurity as one of their strategic priorities. The protection of customers' trust and loyalty is considered a key objective. There are large investments in cybersecurity in this sector and high level of understanding of need for cooperation and collaboration, as well as exchange of information about threats and incidents. ISACs offer a good platform to address the financial sector's needs and this sector is also most active on the European level (FI- ISAC) and worldwide (FS-ISAC). This sector is also highly regulated on the European level (e.g. PSD2 Directive) which obliges operators all over Europe to create and implement security measures.

The **energy sector** is the second most involved in ISACs. Because other sectors are highly dependent on the energy sector, the interdependencies create heightened awareness and realization of how important cooperation and exchange of information is. Therefore, the energy sector is very involved in ISACs not only in Member States but also on the European level (EE-ISAC).

3.2.3 Law enforcement and intelligence community involvement

Law enforcement agencies and intelligence services represent a unique type of governmental entities, due to their special mission. Usually they are not involved in ISACs directly, but have a link to cooperate with them. Direct involvement cannot be achieved due to the large amount of classified information they handle jeopardising the balance of information sharing in an ISAC.

The law enforcement and intelligence community participates in the ISAC as a partner in dedicated sessions.

3.2.4 Cooperation with academia

Some ISACs involve also the academia. This enables the industry to clearly communicate needs in the research and development area. The involvement of the academic community in working groups and ISAC interaction offers also the possibility of creating new solutions useful for critical sectors and overall cybersecurity landscape. For the academia this is a great opportunity for verification of its research in practice.

Academia participates in the ISAC as a partner, often in dedicated open sessions.

4. The Governance Model

The governance model chapter presents approaches on the administration structure and funding options. Governing ISAC is also connected with the objective and procedures, but since both are linked closely to the information sharing process, these are covered in chapter 6.

The overall activity of the ISAC i.e. services delivered, or meetings frequency, is defined by the governance structure. When the secretarial function has been established and a clear structure and managerial roles have been created, the ISAC can launch officially its activities. Workings groups with specific tasks to deliver are set i.e. recommendation, threat analysis. Information sharing is supported by procedures and special tools (e.g. platforms). If on the other hand, the ISAC does not have a clear structure, it is less active and focused on the creation ad hoc voluntary networks of specialists on specific cases. Both ways can be valid and can be adjusted to the needs and availability of the stakeholders involved.

4.1 Common governance structure

ISAC are governed in many ways. Some of them have a clear structure with well-defined roles such as the management board and the secretariat. Others have no structure at all and are very flexible communities where volunteers provide the operating function (e.g. organise meetings).

4.1.1 Structured governance approach

The way an ISAC will be managed depends: some ISACs have a chair and a vice-chair, whereas others choose to have a management board or steering committee. Those roles are rarely elected. Usually professionals that voluntary cooperate in an ISAC perform this function for a specific tenure (a year/two). The ground rule is that the management roles are usually assigned to the private sector or to the entities most involved. When the management roles are assigned, their primary task is to create a strategy for the ISAC development or an action plan which sets up goals and directions of the community. In these structures, elections rules and terms of reference exist.

Examples:

- **Banking Cybersecurity Centre, Poland -** There is a two-level governance structure, involving member representatives: Steering Committee – responsible for establishing strategic objectives and supervision, consists of 9 chosen or elected representatives of BCC members, a member of the Management Board of Polish Bank association and his/her Secretary. Management Group – responsible for participation (e.g. by consultation) in activities aimed at developing organizational and technical solutions; consists of the representatives of all members.
- **Energy European ISAC (EE ISAC)** - The chair is elected by the members of the EE-ISAC as wheel as the members of the board. The chair should come from a utility company. There is no office nor staff. Only an external (non-member) organisation is hired to do the administrative and bookkeeping works.

4.1.2 Governance with supporting body

The role of secretariat is probably one of the most important ones in the governance of ISACs. Thanks to the secretariat, an ISAC could have frequent interactions with a well-set agenda. The secretariat is a facilitator. When the public sector is involved in the ISAC, it usually holds this role. This role is often accompanied by the stimulation of the ISAC.

During the interviews many experts stressed that the role of a secretariat should be permanent, so that the whole ISAC could interact more smoothly. It could be particularly useful for international ISACs to have some public institution fulfilling the role of a secretariat and deal with cultural differences.

4.1.3 Flexible governance

When there is no structure and no defined roles, the ISAC is governed very flexibly, usually by volunteers. One organization/ representative of the organization volunteers to host the meeting; each time another organisation takes the task. Usually in those types of ISACs there is no action plan. Decisions are made ad hoc and to deal with arising challenges. With this flexible governance, meetings usually take place in different locations - offices of different members. It gives the whole community an opportunity to get to know and better understand the organisational culture of other members. The challenge in this case is the lack of formality this ISAC might have and the lack of engagement from the stakeholders.

4.2 Funding options

There are multiple ways for ISAC to obtain funding. An ISAC could be funded by mandatory fees, voluntary contributions as well as with government subsidies. The chart below presents results of the interviews in this area.

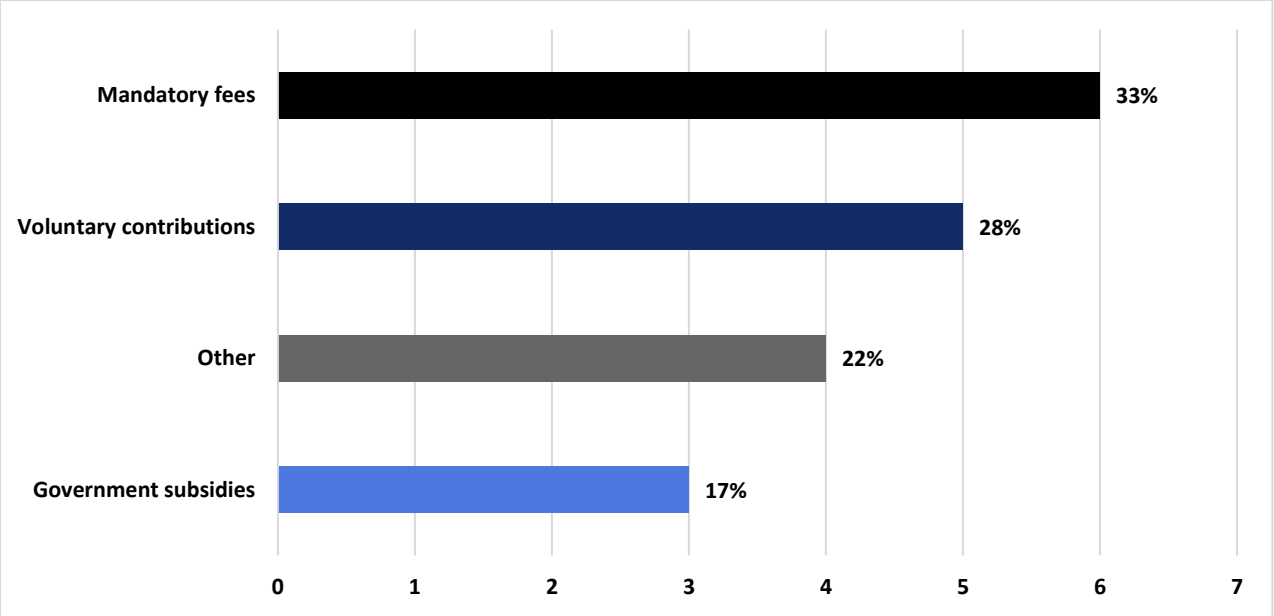


Figure 5 Funding options

Mandatory fees

Mandatory fees are the most common way of funding ISACs. The fee depends on the size of an entity and its involvement in the ISAC. The fees are paid annually and are funding important activities of the ISAC. In some cases, experts believe that the fee creates a motivation for the stakeholders involved to share more information and thus results into active exchange. This is how the Energy ISAC operates.

Voluntary contribution

Voluntary contributions constitute the second most popular funding option. It is not only about budget allocated by members of ISACs, but also about the allocated resources. It could be people who are tasked with working in ISACs, taking part in meetings and working groups or even supporting meetings (events organising, secretariat etc.).

Government subsidies

Government subsidies are usually designated when there is a governmental program or legal framework supporting the ISAC. It is a rather rare funding option, since governments all over Europe believe that this is the private sector's role to secure its services through information sharing. Government subsidies are usually allocated to stimulate and encourage the industry to cooperate, rather than to fund the entire initiative. Government subsidies are often about

facilitation – to operate a secretariat and provide a meeting place. In international or sectoral ISAC this could be the starting point but after the sector becomes more mature a different type of funding is agreed (mandatory or voluntary contribution).

Other

This category is related to the voluntary contribution. It is the case when membership in ISAC is free of charge and everyone contributes by their own time and money. Again: it might be people who are tasked with working in ISACs, and participating in meetings and working groups. It could also be the organisation of a meeting – providing premises and catering.

5. ISAC Capabilities

The core of the ISAC is information exchange; this chapter presents the different approaches to achieve it and presents how trust can be built between members.

5.1 Information sharing

The main goal of information sharing is more the acknowledgement and enumeration than the actual analysis sharing. Some experts also admitted that for smaller organizations and entities with lower cybersecurity sophistication it could be sometimes hard to process all of the information shared via ISACs. This is why the analysis sharing is one of the main challenges in building the ISACs ecosystem in Europe.

In most of the EU countries the information sharing between ISACs members is conducted by following a formalized agreement or a membership agreement. These agreements include the means of exchange and types of information that should be exchanged. It is important to note that public sector might not be able to sign such a document as the experts are found subject to specific laws for public bodies.

Members of ISACs exchange information about **threats, incidents, vulnerabilities, mitigating measures** and also about the **best practices and tools**. The most common tool for exchanging information is a special web portal/platform (following a specific template) and encrypted emails. Also non secured e-mails, to a dedicated group are being used by ISACs. The most important and efficient method are face-to-face meetings. Among the ISACs, there is a common practice to establish so called “circles of trust”. Some information (e.g. technical details about threats and incidents) can be shared widely with all members. Additionally, there is also the internal circle where the shared information is more detailed. Usually people involved in such an internal circle are the management team (or steering committee) with good knowledge of the organization and high(er) level of trust among each other. Most ISACs use the Traffic Light Protocol (TLP) to share information. Some ISACs also receive information from external sources (e.g. IT security companies).

In most ISACs the information is being validated before it is delivered to all members. In ISACs which do not have such a mechanism, usually information is provided through a mailing list so that all members could see who has delivered it.

5.1.1 Types of information to be shared

- Incidents - details of attempted and successful attacks that may include a description of information lost, techniques used, intent, and impact. The severity of an incident could range from a successfully blocked attack to a serious national security situation;
- Threats - yet-to-be-understood issues with potentially serious implications; indicators of compromise, such as malicious files, stolen email addresses, impacted IP addresses, or malware samples; or information about threat actors. Threat information can help operators detect or deter incidents, learn from attacks, and create solutions that can better protect their own systems and those of others;
- Vulnerabilities - in software, hardware, or business processes that can be exploited for malicious purposes;
- Mitigations - methods for remedying vulnerabilities, containing or blocking threats, and responding to and recovering from incidents. Common forms of such information include patches to plug vulnerabilities, antivirus updates to stop exploitation, and directions for purging malicious actors from networks;

- Situational awareness - information that enables decision-makers to respond to an incident and that may require real-time telemetry of exploited vulnerabilities, active threats, and attacks. It could also contain information about the targets of attacks and the state of critical public or private networks;
- Best practices - information related to how software and services are developed and delivered, such as security controls, development and incident response practices, and software patching or effectiveness metrics;
- Strategic analysis - gathering, distilling, and analyzing many types of information to build metrics, trends, and projections. It is often blended with projections of potential scenarios to prepare government or private sector decision-makers for future risks.

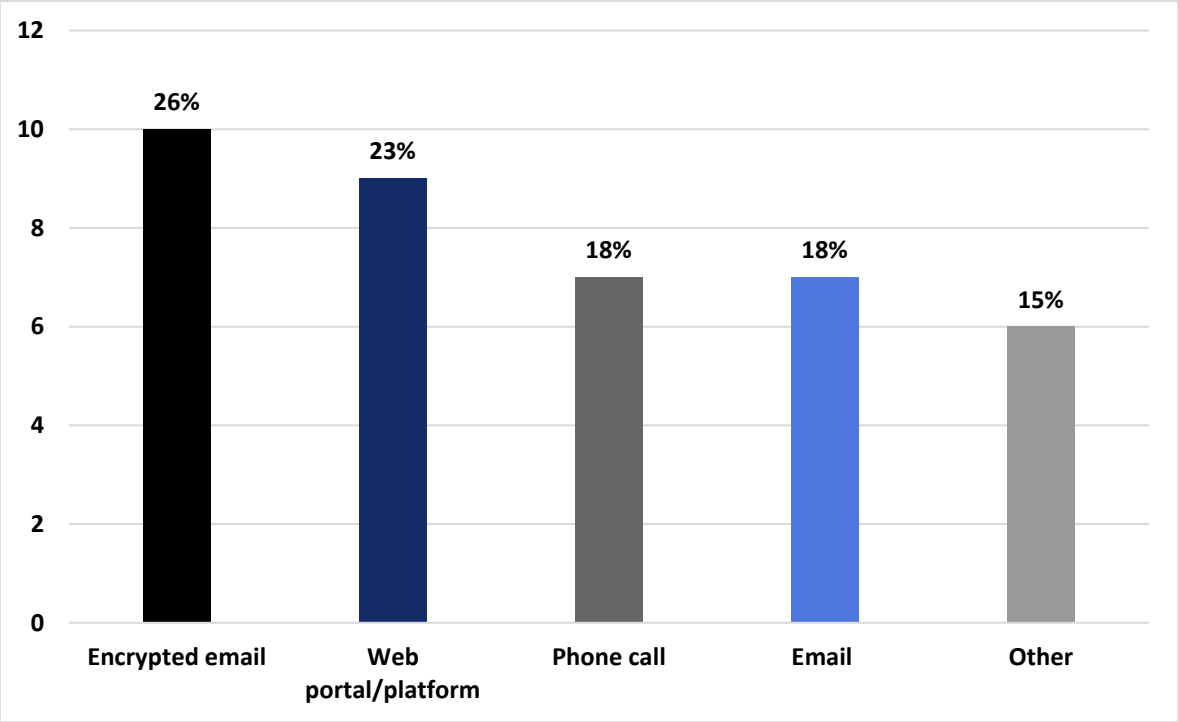


Figure 6 Specific processes and tools used for information sharing in ISACs

5.1.2 Collaboration styles and tools

There is a link between collaboration styles and tools. Collaboration styles (regular meetings, working groups, conferences and side events) determine how often and under which format the ISAC convenes. Additionally, collaboration tools (web portals/ platforms, emails and teleconferences) are strengthening the collaboration by ensuring the way of exchanging information even if the ISAC rarely interacts.

Regular meetings

Based on the findings of this study, regular face-to-face meetings are the most common way for ISACs to interact. They usually take place several times a year (twice a year or quarterly). During these meetings good practices, lessons learnt are presented and topics relevant for the community (presently NIS Directive and GDPR implementation). External experts are sometimes invited, but only to give a presentation about the particular subject. The ISAC community is very careful about inviting external experts to the entire meeting. The reason is that usually during a meeting there are presentations about particular threats and case studies, as well as best practices and lessons learned. These kinds of meetings give members a good opportunity to get to know one another and to network. Example: Sectoral ISAC in NL.

Working groups

This kind of collaboration is a common practice for active ISACs. Working groups are established to deal with particular topics (e.g. botnets). ISAC members delegate experts to work on it so as to provide some solutions/ recommendations for the entire community. Face-to-face meetings are not a must for working groups. They could be quite effective working via emails and teleconferences.

This kind of collaboration offers a good opportunity to prove to other members that the organization is worth cooperating with. The results of the working groups are shared with the community only. Example: FS ISAC.

Ad hoc investigative working group

This kind of collaboration is a reaction to incident/ threats which occurred and is challenging for the community. Ad hoc working groups are formed on a temporary basis to exchange intelligence ad solve the problem. Working groups is a common approach followed by mature ISAC i.e. FS ISAC or NH ISAC (Healthcare ISAC in the US). Working groups can be created ad hoc and maintain a role for a specific mandate or can their existence might cease in case the task has been closed; this depends on the resources available. Example: NH ISAC (US)

Conferences and side events

Annual or ad hoc conferences are organised to raise awareness on the activities of the ISAC and to engage more stakeholders; participation in the conference is open (not only to ISAC members). Sessions that deal with specific technical or relevant policy matters are organised during such conferences allowing an exchange of best practices.

Web portals/ platforms

Most ISACs use this collaboration tool. It allows anonymization of information sharing via ISACs. It also supports the creation of "circles of trust" since not every member gets the same permissions for using the portal/ platform. Another benefit is that some portals/ platforms allow the automation of information sharing. One of the most common tools used is MISP[16].

Emails and teleconferences

These are the most common tools used by ISACs. They are also the way to extend the direct relationship established during face-to-face meetings. PGP keys are usually used to encrypt emails and documents. Also TLP is being used to exchange information. Teleconferences are frequently organised or in exceptional cases when a new threat/vulnerability is disclosed.

5.2 Analysis

As it was mentioned before analysis sharing is one of the biggest challenges for ISACs. When there is too much information in an ISAC, time and resources needed to make analysis increase exponentially. The stakeholders participating in the ISAC perform these activities outside of their working hours, and the analysis of such a vast volume of information requires time and resources.

Many experts interviewed have stated that a team dedicated to make the analysis of all information shared within an ISAC, is currently missing from most ISACs. In some cases, this network should be comprised internally by the member or in other cases, external contractors might offer a solution. Both are challenging – to hire analysts a budget is needed, building a network is very time-consuming. For this reason, most ISACs see the analysis sharing as a future challenge.

Many interim solutions can serve for the analysis task to be realised and formalised; a governmental body can take up this duty. As discussed before, the role that the governmental bodies usually take are the ones of the secretarial

[16] http://www.misp-project.org/

support. In this case however the governmental bodies would have an enhanced role, taking up responsibilities of analyzing information shared. Similarly, on a pan European level, the EU Cybersecurity agency – ENISA – could have this role and assist in the analysis of information on threats, vulnerabilities, incidents etc.

5.3 Trust building

Trust building is a basic element of ISACs and is strongly connected with collaboration styles and tools. If an ISAC interacts often and gives members an opportunity to meet frequently, the level of trust is higher and the overall collaboration and cooperation is better.

Trust plays the key role in the ISACs' success. It is underlined by all experts. The best tool to gain trust is personal relationships. In every single interview, experts pointed out that personal relations are the most important aspect of building trust in an ISAC actually mentioning that after the meeting a social event would help bring the stakeholders closed and get to know each other.

Other mechanisms (besides personal relations) of trust building include:

- Added value: sharing useful information;
- Punctuality: delivering it on time (real time information sharing);
- Comprehensiveness: Delivering good quality reports (clear reports with good information);
- Expertise: Using technical tools (TLP, Terms of reference);
- Dedication: same experts represent their company in each meeting.

This leads to one more issue in the field of trust building. If personal relations are so important, it is a great challenge for an ISAC to continue working smoothly when people change careers. Extension of trust to unknown members is discussed among many ISACs. All experts admitted that even though the best way to build trust is personal relations, it could be also gained using the mechanism mention above. Trust should be tested at all times, if some members have proof that others do not share information as required they should have the right to remove that party from the ISAC (always following a transparent, fair and documented procedure).

There are also formal ways to build the level of trust: first of all, through signing a Non-Disclosure Agreement (NDA), which all members should sign upon confirmation of participation. The NDA should include details like the obligations of the counterparts to the ISAC, the detail of information shared, details about the right use of this information, exclusions from confidential treatment, terms of agreement and penalties in case the NDA is broken. It is recommended that a mutual NDA should be signed to ensure that each side can potentially share confidential information.

A lighter version of a NDA could be the creation of a Code of Conduct; this is a non-legal document which actually provides clear instructions on the standard practice. The most common sections to include are the values and the scope of the ISAC, accountability and liability in case of malpractice, standard of conduct and standard of practice and finally disciplinary actions. Again this should be signed by all potential members of the ISAC.

In the case of face to face meetings Chatham House Rules[17] or TLP[18] should apply and all participants should comply to this requirement (this should be also stated in the meeting minutes and agreed in writing by all participants).

[17] https://www.chathamhouse.org/about/chatham-house-rule
[18] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

Making trust building formalistic might sound like a barrier to actual information sharing, but this kind of formality will only require scrutiny in the initial phases of the creation of the ISAC. All long operating ISACs follow similar approaches and members respect that.

5.4 Capacity building

Some ISACs deliver additional information sharing services to its members. Usually it is because the community has decided that some initiatives could be beneficial and increase sophistication of the industry players participating in the ISAC. Mostly it is vulnerability and/ or threat analysis and training/ exercises. Furthermore, many ISACs that do not deliver such services are considering it, or have already started future planning.

Vulnerability and threat analysis

Vulnerability and threat analysis are delivered mainly by joint contribution. It is done by either creating a working group or assigning tasks to experts from entities participating in ISACs, so that they work jointly and prepare documents that can help whole ISAC. This service was recognised as highly demanding and difficult to deliver, since usually it requires a lot of specialisation and usually involves the best experts. In the same time, most ISACs understand the added value of such services, so the members are willing to bear the costs.

Training and exercises

Joint training and exercises are recognised as important because they support building trust amongst the members and help in overall capacity building by creating expert knowledge. Some entities involved in ISACs even have the rule that every employee should do at least one training per year. ENISA offers such kind of services to the EE-ISAC members.

Exercises organised concern firstly the members of the ISAC, but depending on the maturity level governmental agencies can participate increasing capacity on a national level.

Awareness raising campaigns might also be included in the portfolio of an ISAC but this can still be organized by any kind of PPP. ISAC focus on technical and operational aspects.

6. Establishing an ISAC ecosystem in the EU: future challenges and recommendations

Establishing an ISACs ecosystem would support building security capabilities in Europe. Some member states already understand how useful it is for building resilience on the national level (sector-specific and country-focused ISACs). On the other hand, private sector often states that it is useful to build cross-border partnerships (international ISACs) and exchange information about threats Europe-wide.

ISACs could also be a useful mechanism in the NIS Directive implementation, since they offer an "intermediate level" between essential service operators and CSIRTs on national level. Gathering information about threats and incidents and supporting their members in vulnerability and threat analysis, they can also significantly contribute to the process of risk management (in particular risk assessment) on the national and international level.

The recently published EU Cybersecurity package explains how important the creation of sectorial ISACs is for ensuring a high level of cybersecurity in all 28 MS.

6.1 Challenges

Lack of resources

The biggest challenge for both the public and the private sector is lack of (human) resources. Firstly, because the overall lack of cybersecurity experts on the market, especially in the area of information analysis, but also the high value of the existing resources. Because of this, the industry is not willing to share experts and appoint them to work for ISACs.

Secondly, in the case of the public sector, there are not enough people to support the industry. This concerns not only the secretarial role but also the ability to involve experts who could support the industry on the policy level (e.g. create recommendations, standards)

Weak capacity in analysis role

Because of the overall lack of resources and IT security experts it becomes challenging for ISACs to strengthen its analysis role. Nevertheless, proper (internal) ISAC analysis is defined by the members as essential to the added value of this cooperation model.

Not enough funding

The lack of funding is a general problem for the ISACs. It keeps the member organizations from hiring experts who could work in ISACs themselves, create tools and technical solutions for information sharing and have a permanent secretarial role.

Qualitative evaluation of ISAC activities is difficult

Most of ISACs face the challenge of evaluation. It is difficult to identify clear failure and success factors. For example: Which are the metrics that can measure the cyber security maturity level in a sector after the creation of the ISAC? These are indicators difficult to measure. This relates to the lack of resources and funding, but also to a lack of

cooperation among ISACs on such more abstract level. Meanwhile, the right evaluation process is very important for ISACs to develop and grow.

Duplication of information

It is clearly underlined by experts that due to the existence of many information sharing-groups, the same information is usually passed through different sources. It results in the fact that multiple groups are processing information and acting in parallel. There is often a general lack of coordination.

Inter-ISAC cooperation

Although several initiatives exist of inter-ISAC cooperation (e.g. in the Netherlands the Water and Energy ISAC cooperate on a biannual basis) sharing best practices on areas such as governance and information sharing models, could benefit the development of ISACs in general. By sharing best practices among ISACs, the model will further develop and gain resilience.

The role of regulators and security companies

The role of the regulators or the security companies creates great glitches in the operation of an ISAC. From the one hand the regulators have the power to build legislation based on the information shared and on the other hand the security companies can use it to make business cases. On the other hand, the views of both the regulator and the private company should be heard. A specific type of role should be created for engaging both these actors in a healthy ISAC.

IT tools affecting data integrity

The choice of the right tools to use to ensure data integrity is also a challenge for many ISAC. If the ISAC doesn't have enough funding it is difficult to acquire specialised tools for information sharing and for data analysis. In some cases, ISACs build tools in-house but these kind of solutions are not interoperable and cannot ensure highest level of security. The community however has understood this challenge and more specialised tools are shared between the stakeholders involved (e.g. MISP is offering a complete toolbox for information sharing and analysis).

6.2 Recommendations

Establishing the ISACs ecosystem supports building security capabilities in Europe. Several member states already serve as advocates for building resilience on the national level (sector-specific and country-focused ISACs). Additionally, the private sector mainly advocates to build cross-border partnerships (international ISACs) and exchange information about threats Europe-wide.

ISACs pose as a useful mechanism in NIS Directive implementation, since they can serve as "intermediate level" between essential service operators and CSIRTs on national level. Gathering information about threats and incidents and supporting its members in vulnerability and threat analysis, they can also significantly contribute to the process of risk management (in particular risk assessment) on the national and international level.

Recommendation: ISAC participants (private and public sector) need to invest on trust to ensure the right level of information sharing

Stakeholders need to invest into building trust from the very first steps when creating an ISAC. Pay special attention to each stakeholder's position and requirements. Even with special tools such as platforms and specific procedures, information sharing will not be smooth if there is a lack of trust among members. Because of this, it is essential in the process of creating and stimulating ISACs to establish the right level of trust. Without it, the ISACs will not work properly and stakeholders will not share either information about incidents or the analysis. Give all stakeholders the motivation and the time to invest on the ISAC, and make sure their demands are met equally throughout the collaboration process. Start small, if possible and desirable for consolidating trust bonds. It's very difficult to establish trust within a large group of members, when each member has different interests and motivations. Well established trust relations among some members will spread and pass the right message to others.

Trust is interpersonal and for that reason it is recommended that each ISAC member organisation minimizes replacing the key participants in the meetings. In addition, two persons should represent the member organisation: one permanent representative as well as his/her replacement.

Furthermore, trust is impossible to enforce. So, given the complexity of the cybersecurity threats, a private and public collaborative approach to information sharing is called for. Laws can compel incident reporting, but they do not increase trust or collaboration nor do they reduce risks. Nevertheless, legal studies could be published which encourage information sharing from legal perspective.

Spur voluntary information sharing by building interpersonal relationships. Interpersonal relationships and trust between exchange program participants, along with trust in the program itself, are critical. Reciprocity can be a strong factor in driving cooperation in collective action problem scenarios.

Recommendation: ISAC facilitators need to ensure the right level of attendance for the ISAC participants

It is challenging to have a fruitful discussion when technical people, lawyers and the management are all in the same meeting. It is crucial to have a group of people who 'speak the same language' for the right functioning of ISACs. The right level of attendance also stimulates the involvement and interaction of the members in the ISAC. When everyone speaks the same language, it is easier for them to get involved and share information. When establishing an ISAC, or first meeting, it is recommended to involve or invite the right level of participants.

Recommendation: ISACs should have a structure which motivates the private sector

The structure must address needs and expectations of the private sector, otherwise industry might not join the initiative and not share their information. Since the majority of the NIS sectors are 'owned' by private organizations, their active involvement and support remains essential. Incentives such as leadership positions for the private sector,

or participation in steering committees are a good beginning, but shouldn't be imposed. Having leadership or steering positions defined by equal votes of the members and with a clear mandate (in terms of time and attributions) will legitimate those positions and gather the respect of the members.

Develop an overarching strategy for information sharing and collaboration. An information sharing strategy can help organizations to identify priorities, establish shared values, and set a course for building effective information sharing processes. A strategy can reduce confusion and increase support for information sharing efforts within an organization and among its partners; Creating a strategy from the very first steps of the ISAC including specific objectives and goals, enables the private sector to better coordinate and to plan ahead the investment (in resources) they will invest in the ISAC. Examples might be refunding models for human resource costs. Hence, ISAC activities can be easier done during business hours by experts hired in this position.

Recommendation: ISAC participants should follow the Traffic Light Protocol (TLP) for information sharing

At the very beginning when the trust between members is not well established, the traffic lights protocol is the best way to encourage entities to share information between each other. Maturity in the ISAC will increase the means that are more sophisticated for communication. Focus sharing on actionable threat, vulnerability, and mitigation information. That can create immediate improvements in cybersecurity and can help create better outcomes for ICT consumers in general. Sharing actionable information empowers actors to better defend networks and mitigate threats.

Another type of protocol is Chatham House rules, which can be used during workshops or meetings. Combination of all these codes would be important for trust building.

TLP is an instrument for sharing information within a trusted community, commonly executed by public private cooperation. When public organizations such as police or intelligence are involved, then information sharing might be affected by state-dominated classification models (confidential, secret, etc.). It is important for ISAC members to realize the existence of these differences when setting up rules or terms of reference for information sharing.

Recommendation: The ISAC participants should make sure that the structure engages the public sector

When the public sector gets involved and is active, it stimulates the industry and the process of building ISACs is easier. A good role for the public sector is being the secretariat or being a partner in the ISAC activities. The public sector cannot provide valuable information however as the NCSC model showed before, this is a team work.

Recommendation: Terms of References and a code of conduct should be agreed and signed by all ISAC members

Formal guidelines that are signed by all members support the trust building. There should be common rules agreed by all members, concerning at least the introduction procedure (introducing a new member or organization based on an official procedure), chairmanship and its rotation, and information sharing. In case new organisations join ad hoc specific sessions, NDA’s should be signed.

Information sharing efforts must respect privacy and civil liberties and should be designed with the aim of protecting these to the highest degree. Such efforts should include robust protections built into the exchange and must be based upon Fair Information Practice Principles or other internationally accepted privacy and civil liberties policies.

Recommendation: Every ISAC should produce results periodically

In order for the stakeholders to express the value of the efforts they invest in the ISAC, and to bring new stakeholders in the ISAC, each ISAC could publish results on a frequent basis. Such publications do not have to include confidential

information, but rather lessons learnt and/or recommendations. This makes stakeholders "owners" of a final product, thus giving them more motivation to actively participate and offer more in the community.

Make full use of information shared, by conducting analyses on long-term trends. A greater understanding of the root causes of cybersecurity incidents can help prevent future incidents and can foster improved security analyses. Furthermore, such analyses can also help build knowledge of long-term trends, giving network defenders a better understanding of emerging cyber-threats and of shifts in exploitation methods;

Recommendation: The ISAC participants should agree on the case were mandatory information sharing is required

Mandatory incident reporting is very different than voluntary information sharing. In some instances, such as in the case of national security and public safety, there may be a need for mandatory incident reporting. But such mandatory approaches should be narrowly defined and implemented through trusted mechanisms. This helps ensure that only the right information is shared with the appropriate stakeholders in the proper timeframe. Moreover, such a narrow approach strengthens privacy and the protection of civil liberties. Policy efforts should encourage information sharing processes, which are transparent about how such data is used and which ensure that information shared back to the submitters is valuable and timely.

Recommendation: ISACs governance structure should include the role of a facilitator

It is beneficial when an ISAC has one facilitator, such as a professional secretarial role. This role is responsible for organizing meetings, managing the agenda and keeping track of results, and even stimulating professionalism (such as annual plans). The existence of this role signifies a role of maturity in the ISAC but also establishes a kind of formality.

Recommendation: ISACs should ensure funding mechanisms from their initiation

For an ISAC to grow it is important to secure funding. Then it is possible to set the secretary and resources to deliver good analysis and recommendation. It is also easier to have regular meetings.

Recommendation: The ISAC participants should stimulate cross-sectoral cooperation and work towards it

Some sectors (e.g. finance, energy) are more advanced in the field of cybersecurity. This experience could be used in other sectors as lessons learnt or good practice, and potentially stimulate similar initiatives in other sectors. In some countries this is how ISACs in other sectors have been built and stimulated (e.g. Netherlands).

Recommendation: Law enforcement and intelligence community should have a special role when engaging with ISACs

There is a very thin line when discussing about the involvement or not of the LEA and intelligence communities. This recommendation explains that under specific circumstances, the LEA and Intelligence could be partners to an ISAC and share information in dedicated sessions. Having the forum which allows the cooperation with law enforcement and intelligence community usually appeals to the industry. It gives them an opportunity in the field of fighting against cyber-crime and an opportunity to get information about new threats. There is an overall conviction among the private sector that the government has access to special knowledge, and cooperation could benefit from gathering this information.

Recommendation: The ISAC should perform periodically an evaluation of its activities

It is important for ISACs to be open to evaluation. Members should understand what are the successes and failures of their ISAC, so that the important challenges can properly be addressed. This helps ISACs to grow and evaluate. From the very establishment of the ISAC a long term strategy should be agreed and some initial KPI should be set; throughout time these KPIs might change and become more concrete however the ISAC should set a milestone when the evaluation will take place. This will give the ISAC the opportunity to grow and to reach a more enhanced role in the overall cybersecurity community.

Recommendation: ISACs should develop new services based on the needs of their stakeholders

ISACs should not have in its scope services that already exist in other fora, in order to avoid the feeling of duplicated efforts. If some entity feels that the ISAC will be more a burden then a benefit, they will not join.

7. Next steps: Extension of the role of ISACs

7.1 Evolution of ISACs

There is a significant need for further extension of the role of ISACs. This need is also presented in the recent Communication of the European Commission which requests pan European sectorial ISACs to be created as a way to strengthen cyber security in the EU. It is evident that this kind of collaboration supports trust building and incident/threat information exchange between entities and visibly establish cybersecurity as a priority at national and international level. At the same time, many ISACs look for patterns and additional responsibilities to grow and evolve to be able to also resist more advanced attacks. Below we present some basic ideas that provide the opportunity to further develop the current ISAC model, by focusing on enhanced responsibilities for analysis, outreach/ communications, and capacity/ development.

Analysis: It is evident that the area that requires further development is analysis. ISACs could offer "services related to reducing the impact of an incident and working to restore business functions within the stakeholder". That would be very helpful to members, especially those who have smaller resources. Analysis could be also done by the special "networks of experts" created within the ISACs (consisting of experts selected from ISAC's members).

Outreach: The objective is to "work with the stakeholder to raise the collective understanding of threats that they face and actions that can be taken to reduce the risk posed by these threats". In this task an ISAC could support its members in creating cybersecurity policies and its operationalisation. In addition, an ISAC could offer legal (compliance) consultancy – advising stakeholders about the legal aspects of incident response and new law implementation (e.g. GDPR and NIS Directive). Other valuable means of communication are preparing publications both to a limited audience and to public. The ISAC as a group of more mature stakeholders might even serve as a hub for start-ups and SMEs to gain access to specific experience and knowledge. Through sharing non-sensitive information with other groups or enterprises the ISAC is contributing actively in increasing cybersecurity maturity in a societal level.

Capacity/ Development: ISACs could provide services focusing "on identification, establishment, collection, and analysis of achievement of organizational performance goals, along with measuring organizational effectiveness". That could be special trainings and education programmes, which would enhance members' security culture. This also includes preparing educational and training materials, as well as mentoring programmes where experts from one entity will provide mentoring for experts from another country in given areas. Finally, it might also include preparing plans of developing careers for members' employees.

7.2 The role of ENISA supporting ISACs

In the recent 'Cyber Security Package', published by the European Commission in September 2017, "the Commission will contribute in full to support this approach [of sectorial ISAC] with support from ENISA, with an acceleration needed in particular with regard to sectors providing essential services as identified in the NIS Directive". Taking into account the recommendations and conclusions of this study, ENISA proposes the following:

1. ENISA as a member of sectorial European ISACs: ENISA currently holds membership in the Energy ISAC and at the FI ISAC. In this scheme, ENISA is treated as equal with other members in the community.
2. ENISA as the facilitator of sectorial European ISACs (aligned with the NIS Directive): ENISA holds the secretariat and enables information exchange by providing tools, means and platforms for the stakeholders. In consultation with the Chair, ENISA will be able to organize workshops and support drafting annual activity bulletins. Upon request ENISA might provide expertise on specific topics popular in the community at the time. ENISA certainly will be able to serve as the enabler of cooperation among the different EU ISACs, and foster cooperation.
3. ENISA as independent consultant to European ISACs: ENISA holds the responsibility of providing result-driven information exchange within the ISACs (and if possible among the EU ISACs), thus fulfilling the analysis task of the ISAC. Together with the community, ENISA could issue an internal report for ISAC members that serves as the basis for creating and releasing public information. In this proactive model, ENISA could lead one annual activity in the ISAC (i.e. awareness raising or capacity building).

In order to create and further develop ISACs it is mandatory to build the appropriate level of trust. This enables information sharing, as well as ensuring active involvement of the public sector in the whole process. A European public body like ENISA could play this role and bring all stakeholders together. ENISA regards the recent European Commission proposal as support for gaining and developing this role.

Bibliography/References

Asymmetric Threats, “Strategic Assessment. Engaging Power for Peace”, Institute for National Strategic Studies, National Defense University, March 1998

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG

Electricity Information Sharing and analysis Centre, Understanding your E-ISAC, June 2016, http://www.nerc.com/pa/CI/ESISAC/Documents/Understanding%20Your%20E-ISAC_June%2028%202016_FINAL.PDF

European Distribution System Operators for Smart Grids, Network and information security (NIS): Recommendations for information sharing and risk management, September 2014, https://www.edsoforsmartgrids.eu/wp-content/uploads/public/EDSO-recommendations-on-Network-and-Information-Security-NIS-September-9-20141.pdf

Executive Order -- Improving Critical Infrastructure Cybersecurity, February 2013.

Federal Ministry of Interior, National Plan for Information Infrastructure Protection, Bindesministerium des Innern, October 2005

Francy F., The Aviation Information Sharing and Analysis Center (A-ISAC), April 2015.

FS-ISAC, Established by Financial Institutions, FSARC Deepens Analytic Capabilities to Combat Cyber Risk and Strengthen Resiliency of U.S. Financial System, FS-ISAC ANNOUNCES THE FORMATION OF THE FINANCIAL SYSTEMIC ANALYSIS & RESILIENCE CENTER (FSARC), 2016, http://www.fsisac.com/

FS-ISAC, Financial Services Information Sharing & Analysis Center FS-ISAC Operating Rules, June 2016, https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_June2016.pdf

Goodwin C., Nicholas P.J., A framework for cybersecurity information sharing and risk reduction, Microsoft, 2015, https://www.microsoft.com/en-us/download/details.aspx?id=45516

Hielke Bontius, Advancing cyber security Nationally and internationally, January 2017

Jeong Ch., Ahn S., National Cyber Threat Information Sharing System Strengthening Study, Contemporary Engineering Sciences, Vol. 7, 201, December 2014, http://www.m-hikari.com/ces/ces2014/ces29-32-2014/20jeongCES29-32-2014.pdf

Johnson Ch., Badger L., Waltermire D., Snyder J., Skorupka C., Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150, October 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Jorge Valero, Europe struggles to tackle cyber attacks in aviation, EURACTIV.com, https://www.euractiv.com/section/aviation/news/europe-struggles-to-tackle-cyber-attacks-in-aviation/

Luiijf E., Kernkamp A., Sharing Cyber Security Information Good Practice Stemming from the Dutch Public-Private-Participation Approach, March 2015, https://www.thehaguesecuritydelta.com/media/com_hsd/report/40/document/Sharing-Cyber-Security-Information-GCCS-2015.pdf

National Council of ISACs, The Reach of Information Sharing and Analysis Centers, January 2017, https://www.nationalisacs.org/publications

National Cyber Security Centre in Netherlands, ISACS's, https://www.ncsc.nl/english/Cooperation/isacs.html

OECD, Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, 2012, https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Prieto P. D, *Information Sharing with the Private Sector: History, Challenges, Innovation and Prospects*, 2006, https://www.files.ethz.ch/isn/90165/2006-09-15_Seeds-of-Disaster.pdf

UNICRI with support of Cyber Security Center, Working Paper Information Sharing and Public-Private Partnerships: Perspectives and Proposals, 2013, http://www.combattingcybercrime.org/files/virtual-library/national-laws/information-sharing-public-private-partnerships,-perspectives-and-proposals.pdf

Weiss, N. E., Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis, Congressional Research Service, June 2015, https://fas.org/sgp/crs/misc/R43821.pdf

World Economic Forum, Guidance on Public-Private Information Sharing against Cybercrime, January 2017, http://www3.weforum.org/docs/WEF_Guidance_Cybercrime_report_2017.pdf

Annex A: Overview of ISAC in the EU

Country	Austria
Cybersecurity system (main institutions)	Fenderal Chancellory, Ministry of Interior, CERT.Gov, national CERT
ISACs	the Austrian Trust Circle (ATC) https://www.cert.at/about/atc/content.html

Country	Belgium
Cybersecurity system (main institutions)	CERT.be Cybersecurity Centre
ISACs	CTISRP (Cyber Threat IntelligenceResearch Project) Cyber Security Coalition BELNIS (Belgian Network and Information Security)

Country	Bulgaria
Cybersecurity system (main institutions)	CERT Bulgaria Minitry of Infrastructure
ISACs	BAIT (Bulgarian Association of Information Technologies)

Country	Croatia
Cybersecurity system (main institutions)	National CERT
ISACs	-

Country	Czech Republic
Cybersecurity system (main institutions)	CZ.NIC https://www.nic.cz/ National Security Authority
ISACs	-

Country	Cyprus
Cybersecurity system (main institutions)	National CERT
ISACs	-

Country	Denmark

Cybersecurity system (main institutions)	Centre for Cyber Security, Council for Digital Security
ISACs	-

Country	**Estonia**
Cybersecurity system (main institutions)	Information System Authority https://www.ria.ee/en/ CERT Estonia
ISACs	-

Country	**Finland**
Cybersecurity system (main institutions)	National Cyber Security Center (NCSC-FI) https://www.viestintavirasto.fi/en/cybersecurity.html FICORA
ISACs	FI-ISAC, NCSC-FI, Following sectors are active in Finland: Food supply, Healthcare, Finance, ISP/telecom, Energy, Government, Software Vendors, Vulnerability research, Media

Country	**France**
Cybersecurity system (main institutions)	ANSSI (The National Agency for the Security of Information Systems) CERT.FR
ISACs	Club des directeurs de sécurité des entreprises

Country	**Ireland**
Cybersecurity system (main institutions)	CERT within one of the Ministry
ISACs	Infosecurity Ireland, Ireland Chapter

Country	**Italy**
Cybersecurity system (main institutions)	CERT
ISACs	AIIC (Associazione italiana esperti in infrastructure critiche)

Country	**Greece**
Cybersecurity system (main institutions)	Ministry of Digital Policy NCERT-GR was established in 2009. It is responsible for coordinating incident response measures for both government institutions and entities engaged with critical public infrastructure. The Assurance Authority for Confidentiality of Communication (ADAE) acts as the primary body responsible for network and information security in Greece. The

	National Intelligence Service of Greece (NIS) handles matters related to information and network security as outlined in Law 3649/2008. These duties include the administration of NCERT-GR, the national CERT. There is not, however, a body or agency within the NIS dedicated to network and information security — apart from the limited, response-focused scope of NCERT-GR. The Directorate of Cyber Defense, reporting to the Chief of Defense is responsible for cyber warfare and liaises with the NIS and the Greek police services. The Greek Cybercrime Centre is a national project aimed primarily at improving research and education in the area of cyber attacks. It does not handle network and information security at large.
ISACs	NCERT-GR is responsible for the collection of cybersecurity incident data. It maintains an emailed-based reporting platform to log cybersecurity incidents.

Country	**Germany**
Cybersecurity system (main institutions)	BSI (Federal Office for Information Security) National CERT CERT-BUND
ISACs	UP KRITIS (Kooperation zwischen Betreibern Kritischer Infrastrukturen)

Country	**Hungary**
Cybersecurity system (main institutions)	National Security Authority Cyber Security Centre CERT-Hungary
ISACs	ISCD (Conference on Information Security and Cyber Defence)

Country	**Latvia**
Cybersecurity system (main institutions)	CERT.LV
ISACs	DEG (Information Technology and Information Systems Security Experts Group)

Country	**Lithuania**
Cybersecurity system (main institutions)	CERT-LT State Information Resources Management Council
ISACs	Forum of the information exchange - voluntary community

Country	**Luxemburg**
Cybersecurity system (main institutions)	GOVCERT.LU https://www.govcert.lu/en/ Luxembourgish Cyber Security Board http://www.gouvernement.lu/
ISACs	CERT.LU – all the CERTs from the Luxemburg (https://www.cert.lu/) CIRCL https://www.circl.lu MISP – system (http://www.misp-project.org/)

Country	Malta
Cybersecurity system (main institutions)	MITA (The Malta Information Technology Agency) CSIRT Malta
ISACs	-

Country	The Netherlands
Cybersecurity system (main institutions)	National Cyber Security Centre https://www.ncsc.nl/english
ISACs	In the Netherlands the following sectors are active: Ports, Airports, Financial Institutions, Water Management, Multinationals, Telecom, Nuclear, Healthcare, Energy, Drinking Water, Managed Service Provider (MSP), Insurance and the National Government and Pensions. The chairmen of the various ISAC's meet up in a number of sessions every year to discuss the overarching themes with the sector. There are also: Liaison officers; ICT Response Board; National Response Network, National Detection Network, Operational Incident Response Team network, 'Ecosystem' projects trade nexuses Port of Rotterdam and Schiphol Airport.

Country	Poland
Cybersecurity system (main institutions)	Ministry of Digital Affairs Ministry of Internal and Police Department NASK – National Cybersecurity Center, CERT Polska Internal Security Agency – CERT.GOV.PL
ISACs	Banking Cybersecurity Centre (BCC) CERT in Energy sector (PSE and Energa) Network Security Incident Exchange ABUSE Forum

Country	Portugal
Cybersecurity system (main institutions)	Centro Nacional de Cibersegurança CERT.PT
ISACs	National Cyber Security Center National Network of CSIRTs https://www.cncs.gov.pt/en/cooperation/national-network-of-csirts/ http://www.cert.rcts.pt/index.php/rede-nacional-csirt/directorio

Country	Romania
Cybersecurity system (main institutions)	CERT-RO Intelligence Authority - CIP
ISACs	CCSIR (Cyber Security Research Center from Romania)

Country	Slovenia

Cybersecurity system (main institutions)	SI-CERT
ISACs	

Country	**Slovak Republic**
Cybersecurity system (main institutions)	CSIRT.SK Ministry of Finance National Security Authority http://www.nbu.gov.sk
ISACs	

Country	**Spain**
Cybersecurity system (main institutions)	CNPIC (National Centre for Critical Infrastructure Protection)
ISACs	ICARO – critrical infrastrycture protection Foro ABUSES, CCI (Industrial Cybersecurity Centre)

Country	**United Kindom**
Cybersecurity system (main institutions)	Department for Culture, Media & Sport – Digital Economy Minister National Cyber Security Centre https://www.ncsc.gov.uk/ Office of Cyber Security and Information Assurance https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
ISACs	-

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-07-17-050-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-239-4
DOI: 10.2824/549292