ENISA'S OPINION PAPER ON ISAC COOPERATION

March 2019

ENISA presents its views on how ISACs strengthen EU cybersecurity and identifies the benefits of ISACs to the Digital Single Market.

INTRODUCTION

As cooperation is a *sine qua non* for ensuring cybersecurity, the European Union is a strong advocate of cooperation models in cybersecurity. The European Commission demonstrates its support through developing EU regulation such as the Cybersecurity Act[1], the recently launched Proposal for a European Cybersecurity Competence Network and Centre[2], and initiatives under the umbrella of the Connected Europe Facility[3]. EU public and private stakeholders look to ENISA, as the EU Agency supporting these EU focused cybersecurity activities.

In this brief paper, ENISA will share its opinion on the ongoing developments and traction of Information Sharing and Analysis Centers (ISACs). The ISAC-model has demonstrated its value to cyber experts, policy advisors and managers in EU Member states such as the Netherlands where the National Cyber Security Centre actively supports ISACs, and in sectors such as finance where ISAC cooperation exists for many years on pan European, international and national level.[4]
The EU institutions, Member States and industry are increasing their interest in ISACs as a cooperation model: Organisations such as the European Cyber Security Organisation (ECSO) and the European Commission support the model by exploring financial programmes such as the Connecting Europe facility (CEF), discussing possibilities for cooperation, and suggesting further investment through procurement.

[1] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[2] https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

[3] https://ec.europa.eu/inea/en/connecting-europe-facility

[4] https://www.ncsc.nl/samenwerking/_samenwerken/sectorale-samenwerking-isac.html

ENISA has supported EU-ISACs for many years and in different roles varying from assisting the development to the active membership in EU ISACs. Why this paper at this moment in time? As this model is not regulated in the EU and its cooperation is voluntary, ENISA considers the ISAC approach as a solid cooperation-model to explore and build upon. Supported by the new ENISA mandate and regulation that tasks ENISA to further invest in ISACs, ENISA is motivated to promote the ISAC-model among the EU member states and industry because:

- The model focuses on cooperation across borders and sectors at a time where the EU is introducing multiple regulatory cybersecurity focused initiatives and ENISA is in the unique position to bring together the required public and private knowledge and expertise;

- The model allows for multi-layer cooperation from discussing strategic issues to operational challenges;

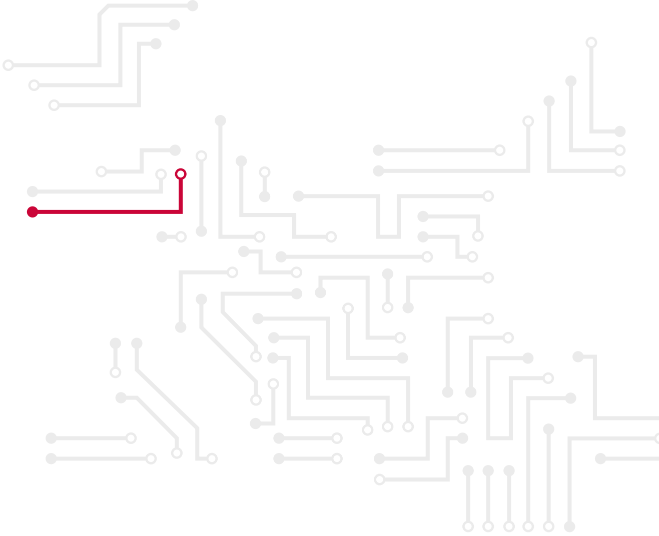
- The model requires no 'heavy' EU regulatory framework, but simply the willingness of cooperation and sharing based on trust, equality and transparency among Network and Information Security (NIS) experts;

- The model increases cybersecurity information sharing at national level.[5]

Therefore, the ISAC-model deserves more public justification and support.

In this paper, ENISA presents its views on how ISACs strengthen EU cybersecurity and identifies the benefits of ISACs to the Digital Single Market.[6] As the ISAC model receives growing support and in order to avoid fragmentation, ENISA concludes with some recommendations on the future development of ISACs within a European context. The target audience of the paper consists of policy makers as well as critical infrastructure and industry representatives that are already involved in sectoral cooperation such as an ISAC, and/or are interested in learning more about ISACs.

Supported by the new ENISA mandate and regulation that tasks ENISA to further invest in ISACs, ENISA is motivated to promote the ISAC-model among the EU member states and industry.



[5] In the Netherlands, the ISACs are considered to be an essential instrument in strengthening the resilience of critical infrastructure sectors, and by doing so supportive of the NIS Directive. ISACs have contributed annually to the National Cybersecurity Assessments: https://zoek.officielebekendmakingen.nl/blg-811523.pdf
In the UK, the CiSP model is similar: https://www.ncsc.gov.uk/cisp

[6] In 2018 ENISA published a study on analysing EU models and how EU ISAC's work: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

1. BACKGROUND OF ISACs

Information Sharing and Analysis Centres (ISACs) provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) and offer active sharing of information between the private and the public sector. ISACs have created communities within the private and governmental sector. 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. One of the main recommendations was to establish Information Sharing and Analysis Centres (ISACs) in order to build and strengthen cooperation between public administration and the industry.[7]

Recent analysis and research shows that information sharing through ISACs is effective and creates an ecosystem in which trust is being built among critical operators.[8] This allows entities less advanced in the field of cybersecurity to learn from others.

[7] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

[8] Luijf E., Kernkamp A., Sharing cyber Security Information Good Practice Stemming from the Dutch Public-Private-Participation Approach, March 2015: https://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf
Huistra A. W., Krabbendam-Hersman T.H.E.E.A., Exploring Cybersecurity Information Sharing among Top Sectors (Netherlands), March 2017: https://www.rijksoverheid.nl/documenten/rapporten/2017/03/07/verkenning-cybersecurity-informatiedeling-binnen-de-topsectoren

2. EU STATE OF PLAY: ISACs

European legislation encourages the creation of ISACs: the NIS Directive supports incident reporting and the EU Cybersecurity Act proposal supports information sharing and analysis sharing among public and private entities in an effort to ensure cybersecurity. ENISA should support information sharing in and between sectors, in particular in the sectors listed in Annex II of the NIS Directive, by providing best practices and guidance on available tools, procedure, as well as providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral ISACs.[9]

Under the Connecting Europe Facility (CEF) funding, several objectives are defined to establish an enabling facility for a series of European level sectoral ISACs (Information Sharing and Analysis Centers) with industry and NIS Directive stakeholders for improved awareness and preparedness of cybersecurity risks and threats.[10] It demonstrates the support of the European Union to invest in the ISAC model on European level.

ENISA is actively involved in the creation and development of EU focused ISACs. The Agency supports the EU Energy ISAC, the EU FI ISAC, and the development of the EU Aviation ISAC and EU Railway ISAC.

ENISA's membership offers the ISAC its experience in capacity building and technical expertise such as analysing incidents and threat intelligence. In addition, ENISA offers its extensive network to further support the ISACs. Each ISAC has its own development process and characteristics, which means that ENISA adjusts its role accordingly.

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_12058_2018_INIT&from=EN

[10] https://ec.europa.eu/digital-single-market/en/news/connecting-europe-facility-supports-expansion-cybersecurity-capabilities

3. THE BENEFITS OF COOPERATION

The European Union is responsible for suggesting and driving initiatives that lead to cooperation in cybersecurity. The NIS Directive, the Cybersecurity Act including the certification proposal, and the recently published proposal for a European Cybersecurity Competence Network and Centre, reflect this. Although it is essential that public institutions initiate necessary cyber regulation, it is important to mention that administrative and regulatory thinking must not become counterproductive to cybersecurity cooperation and the digital market. It is unavoidable that independent initiatives to secure and strengthen models such as ISACs might create ambiguity among the (potential) stakeholders. This is why ENISA recommends that the industry takes the lead in creating sectoral ISACs, supported by ENISA. In the absence of industry not taking initiative, the public sector could fill the gap. These initiatives strengthen the autonomy of the stakeholders involved, create the opportunity to invite the public stakeholders like law enforcement, and ultimately build the foundations for an ISAC based on trust, equality and shared interests.

Public private cooperation is at its best when the stakeholders cooperate based on common interests, not on differences. The same argument applies to the EU institutions active in cybersecurity. A future network of multiple EU focused ISACs could create a strong network of defence to protect the digital society and our Digital Single Market. ENISA is committed to fulfil this responsibility together with the relevant public and private stakeholders.

National cybersecurity authorities will benefit from supporting ISACs at national and EU level because it will not only provide them access to the industry, it will also provide them with a platform to informally discuss incidents, threats, and policy proposals.

4. KEY MESSAGES/ RECOMMENDATIONS

The ISAC model represents great potential for strengthening cybersecurity and resilience in the European digital society. In February 2018, ENISA published a comprehensive study on the different cooperation models of ISACs.[11] Its conclusions and recommendations explain the functioning and potential value of ISACs to relevant stakeholders. In this opinion paper, ENISA further elaborates on this study by providing concrete recommendations to our stakeholders with the purpose to promote and point out the future potential of EU level ISACs and their cooperation:

a. ENISA supports existing EU ISACs that represent critical infrastructure. However, not all Operators of Essential Services (OES) sectors are represented with an ISAC on the EU level. ENISA therefore strongly recommends OES active on the EU market that are not yet in an ISAC, to explore and initiate cooperation by following the ISAC-model. Several national cybersecurity authorities in the EU have already developed a strong model of ISAC cooperation. ENISA welcomes these initiatives and advises OES to get informed and become involved on both a national and European level if possible.[12]

[11] Refer to footnote 4.

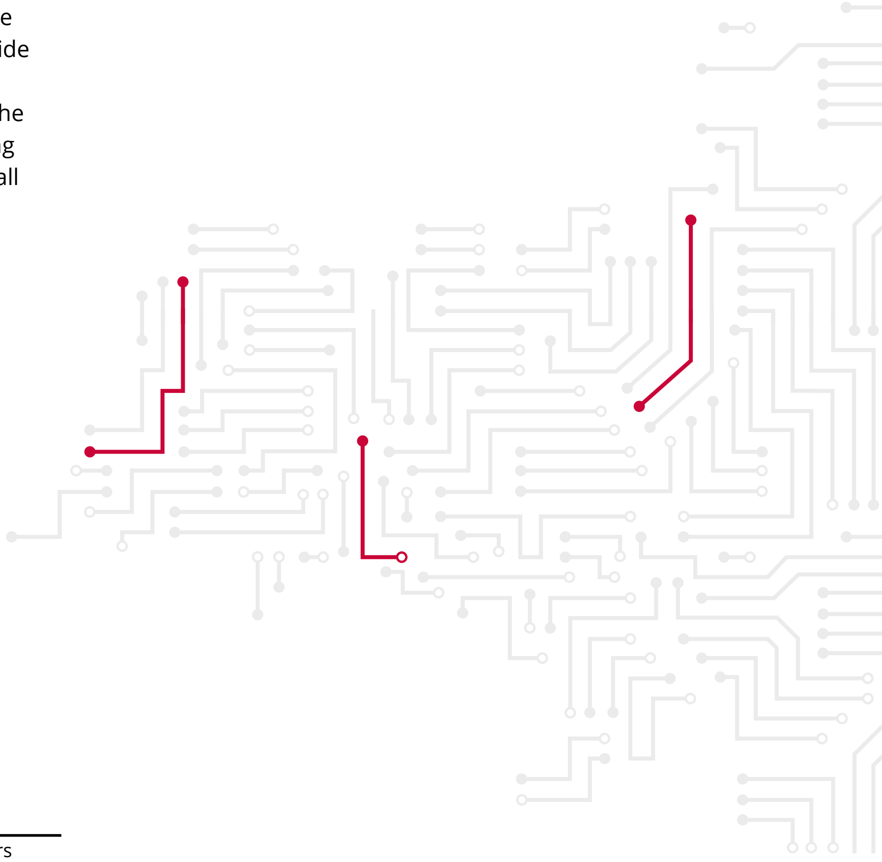
[12] https://www.enisa.europa.eu/news/enisa-news/enisa-releases-online-nis-directive-tool-showing-per-sector-the-national-authorities-

b. Although the initiation of an ISAC model remains voluntary, this process requires expertise and existing knowledge of cybersecurity cooperation. This is especially a concern for EU focused ISACs. The challenge of organising or facilitating ISAC cooperation within the context of EU Member States and its institutions requires up-to-date knowledge of the current possibilities and existing proposals. ENISA recommends any newly formed EU focused ISAC or related collaboration initiative to find a sponsor with excellent knowledge of EU institutions and funding opportunities in order to become accepted as the ISAC representing the sector.

c. It is recommended that the current EU focused ISACs continue to develop their activities with the support of EU institutions, engaging and sharing knowledge amongst each other. Against the background of recent EU regulation that refers to cybersecurity cooperation there is a continuous need for cooperation concerning cross-sectoral dependencies, this is a clear opportunity to further mature and professionalise. In particular, ENISA recommends to invest in developing the analysing capabilities within and among the existing EU focused ISACs. By sharing their best practices, analysis and expertise, ISAC members hold great potential for addressing cross-sectoral challenges.

d. EU focused ISACs represent not only an opportunity to gather public and private stakeholders to share their information and analysis, but once ISACs are operational and ready to share information outside their organisation, ENISA recommends exploring cooperation with CSIRT communities, and even the European CSIRTs Network. Thus, creating a strong network of relevant players potentially covering all relevant operators of essential services.

e. Lastly, ENISA recommends initiating the discussion on the development, structures and direction of EU focused ISACs. What is desirable in terms of representation of OES in EU focused ISACs: representation per member state, or representation by industry and multinationals? Should EU focused ISACs be an instrument where more mature OES stakeholders inform and assist the less mature OES stakeholders in the EU cyber ecosystem? Is there a maximum span of control concerning the amount of members? How do the relevant stakeholders in the EU ISAC ecosystem ensure that collaboration benefits all involved? ENISA advises to initiate this discussion in order to assist the next generation of collaboration.



for-operators-of-essential-services-and-digital-service-providers

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 media enquires about this paper, please use press@enisa.europa.eu.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This ublication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

Vasilissis Sofias Str 1
151 24 Maroussi, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu