The European Cyber Shield

Otmar Lendl <lendl@cert.at>

2023-09-12
Version 1.0
[TLP:CLEAR]

As part of the EU Cyber Solidarity Act, which the EU Commission proposed on 18 April 2023, the concept of the "European Cyber Shield" was published. This document is my attempt to explain the ideas behind the Cyber Shield and offer a few suggestions on how Chapter 2 of the **proposed Cyber Solidarity Act can be improved.**

Disclaimer: While I tried to get feedback from all relevant stake-holders, this is still my personal opinion and not the official Austrian position on this subject.

Executive Summary

The proposed Cyber Shield (Chapter 2 Cyber Solidarity Act) contains valid ideas: supporting SOCs by fostering national and cross-border collaboration is worth doing.

An unfortunate choice of terminology is prone to confuse readers of the Act. A change would be welcomed.

The relationship between the proposed structures and the tasks of the CSIRTs and the CSIRTs network (as stipulated in the NIS2 Directive) is not entirely clear. Defining this relationship and integrating the proposed roles with the existing structures would be useful.

EU funding for multiple consortia with the aim of building closer, technical collaborations in cross-border structures is a sound investment.

Content

Terminology

First, we need to clear up the relationship between the CSIRT, SOC and ISAC concepts.

CSIRTs

While the literal meaning of the acronym ("Computer Security Incident Response Team") centers on Incident Response, the CSIRT Services Framework defined by FIRST.org (in collaboration with TF-CSIRT and the ITU) describes a much broader spectrum of services that CSIRTs provide. These range from Detection, Incident Response (IR), Vulnerability Mangement, Situational Awareness to Knowledge Transfer. Not every team has the same focus; the actual task fulfilled varies a lot between teams. In the case of national CSIRTs[1], additional task are relevant like acting as the social hub for the national cyber security community. The FIRST Services Framework also introduces the concept of a Coordinating CSIRT and notes that *"Today, national CSIRTs have been established as a distinctive type of Coordinating CSIRT to facilitate and often coordinate the activities of CSIRTs located in a particular nation or offer limited services for all citizens, specific sectors of critical infrastructure entities, etc. of this nation."*

It is important to note that "detection" and enabling "information sharing" can be core tasks of national CSIRTs.

The term National Cyber Security Centres (NCSCs) is often used to make clear that the national CSIRT has grown far beyond pure Incident Response.

In addition to "CSIRT", other terms are also used to describe the same concept. The use of "CERT" ("Computer Emergency Response Team") is also popular, but due to it being a registered mark of Carnegie Mellon University, legal texts use the acronym CSIRT (early drafts of the NIS 1 directive used "CERT"). There is no universally accepted difference in meaning between "CERT" and "CSIRT", I use the terms interchangeably.

SOCs

There is no universal definition of a Security Operation Center (SOC). Furthermore, the meaning of the term is evolving.

Wikipedia: The job of a Security Operation Center is the protection of an organization against cyber threats by establishing visibility into the operation of its IT systems, monitoring for signs of intrusions and following up on any such hints. This can include full Incident Response capabilities. It comprises both people, processes, and technology.

Mitre (2014): A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Mitre (2022): A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents.

SANS (2018): A combination of people, processes and technology protecting the information systems of an organization through: proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state, and minimizing damage from unwanted effects.

[1] In the EU context, "national CSIRT" should be read as "CSIRT in a Member State that has been designated under the national transposition of the NIS-D's Article 9 or NIS2-D's Article 10 respectively". More on the definition of a national CSIRT can be found here: https://cert.at/en/blog/2018/8/blog-20180731155524-2252

SANS (2020): The core functions of a SOC are: collection, detection, triage, investigation, incident response.

McAfee (2013): The SOC is responsible for monitoring, detecting, and isolating incidents and the management of the organization's security products, network devices, end-user devices, and systems.

Trellix: Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Information Security Asia: A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents and threats. It serves as the nerve center for an organization's cybersecurity operations, providing real-time monitoring, incident response, and threat intelligence gathering.

For me, the core mission of a SOC is monitoring and detection. There is an aspect of prevention, especially as EDR (Endpoint Detection and Response) solutions are picking up the capability to prevent suspicious activities. On the other side, a detection of an anomaly needs to be investigated and if verified as malicious, contained and remediated. Some commercial SOC providers thus call their service "Managed Detection and Response".

Others (e.g. CCN/RNS) see the SOC as the unit in an organization that combines all the Cyber Security functions (it is the "center" after all), including prevention, protection, detection, response and the overarching security management.

There is no need to agree 100% on one single universal definition a "SOC". We just need to be sure we think of the same functions when reading the EU Cyber Solidarity Act. Nevertheless, I think we need to agree that a SOC must at least process raw log data from a network infrastructure in order to detect an attack or breach.

ISACs

Information Sharing and Analysis Centers (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 about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.

Many national CSIRTs (in the NIS context) run ISACs for national constituency-groups. These are often organized by sector. The various CSIRT associations can also be considered special cases of ISACs. National and sectoral CSIRTs are also often involved in sectoral ISACs on an international level.

Commonalities

The definition and task description of both CSIRTs and SOCs contain detection and response capabilities. The primary focus might be different (SOCs centring on detection, CSIRTs on response), but their jobs are far from being free of overlap.

A SOC will move into IR territory every time the sensors and the logic behind them detects an anomaly. This response will hopefully result in determining that the alert was a false positive. Nevertheless, the steps taken to confirm this are typical Incident Response procedures.

Conversely, when a Security Incident Response team is called to handle a live incident, one of the first steps to be done is to establish visibility – basically establishing SOC functionality.

Both detection and response need cyber threat intelligence (CTI) and generic situational awareness to perform their tasks. The SOC needs to know the tools, tactics and procedures (TTPs) of adversaries in order to build and tune detection capabilities, and during an IR it is also essential to know what the responders are dealing with and how the threat actor operates.

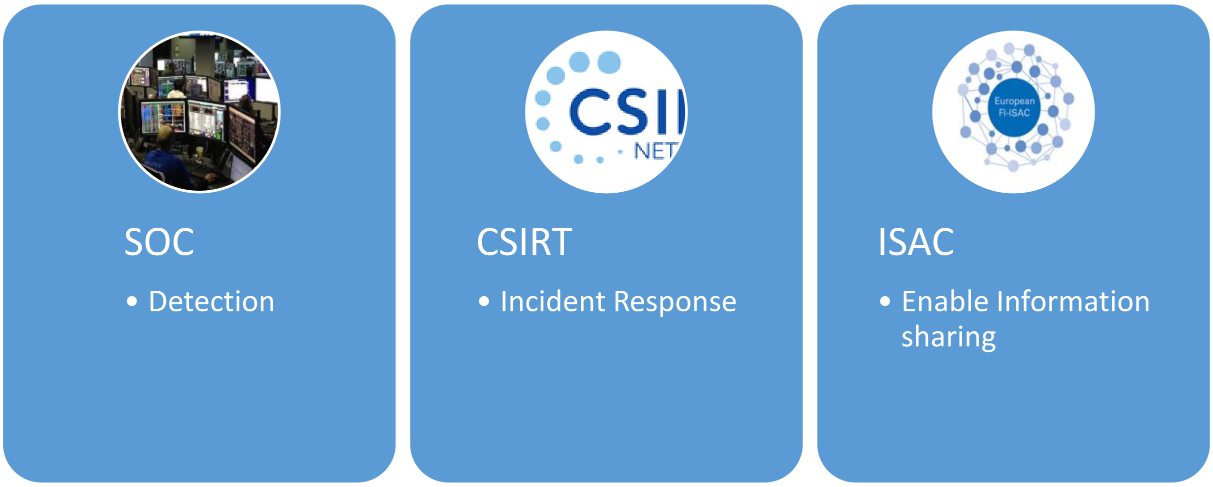
This information (situational awareness and CTI) is also at the core of what ISACs are all about: Information that helps participants be better at prevention, detection and response.

Prevention – Detection – Response – Information Sharing

Therefore, it would be helpful if the language in the EU Cyber Solidarity Act decreases its reliance on on the SOC/CSIRT/ISAC terminology with its overlapping definitions, and instead focusses on the functions and/or tasks that the various entities perform.

Facets, not Silos

Following various EU documents and initiatives (NIS1 doesn't not mention SOCs or ISACs, NIS2 only has one reference to a SOC; the Empowering EU ISACs project did not liaison with the CSIRTs Network; and Recital 15 of the CSoA contains language like "The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network") one can get the impression that SOCs, CSIRTs, and ISACs are independent entities, each in its own silo:



SOC

- Detection

CSIRT

- Incident Response

ISAC

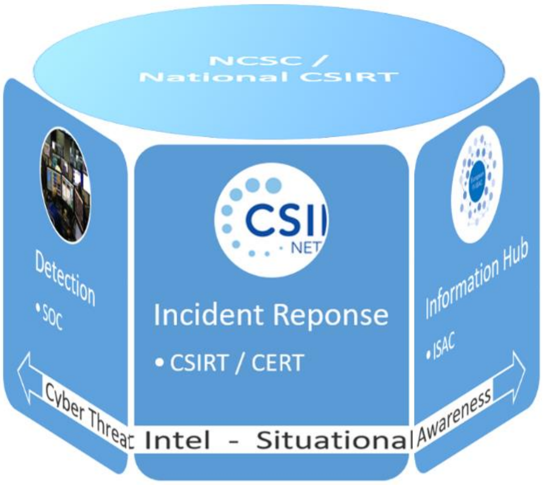
- Enable Information sharing

This is misleading. Many national CSIRTs include SOC functionality (e.g. via a national sensor network[2], or because they operate a government network SOC[3]) and they run ISACs. They perform all three functions – and probably more like national awareness campaigns, active cyber defense, community building, etc.

A much better visualization is to see these functions as facets (or roles, tasks) of CSIRTs: depending on the occasion and the point of view, the NCSC / national CSIRT can look like a SOC, an IR function or the manager of (or participant in) an ISAC. Visually:

[2] E.g. the NCSC-NL and the Dutch NDN, NCSC-FI and HAVARO, Latvia, Denmark, Norway, …

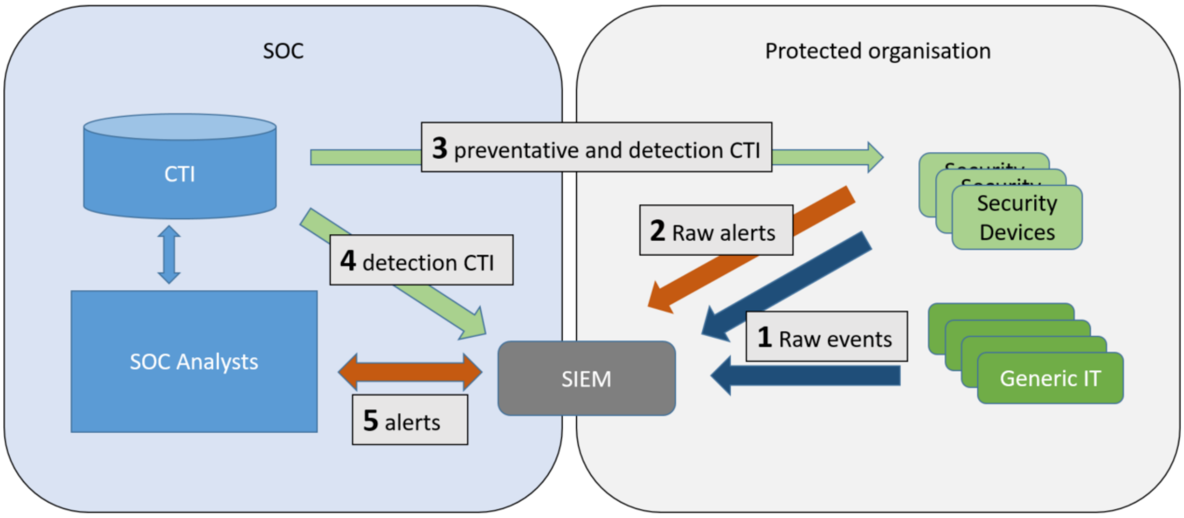
[3] E.g. BSI's "Bundes Security Operations Center" (BSOC)



For example, the teams in the CISRTs Network (CNW) have been sharing indicators concerning recent spear phishing campaigns by multiple threat actors. In a way, the CNW is acting as ISAC of the EU national CSIRTs. The information shared is useful for prevention, detection and response; it thus does not neatly fall in either category. Some of the CNW members can directly use these indicators for detection purposes (e.g. in a national sensor network, or as part of their SOC role for government IT systems), others need to pass them on to the security teams of their constituents.

Data flows

In order to explain the implication of some of the ideas in the Cyber Solidarity Act, we need to look at the data flows between the various systems and actors. The following diagram is a simplified version of the relationship between a SOC and the organization it is tasked to protect. The SIEM (Security information and event management) can be both on premise or located at the SOC (or in the cloud). The SOC needs a good (up-to-date, precise and comprehensive) collection of Cyber Threat Intelligence[4] (CTI). Commercial vendors are one possible source, some CTI is available from open sources, some can be obtained from peers (SOCs, CSIRTs, e.g. via ISACs), and some will be derives in-house from prior incidents.



[4] See https://cert.at/en/blog/2023/9/cti-data-feeds for a classification of CTI feeds.

The relevant information flows are:

1. Raw events from the IT systems towards the SIEM. This is basically an implementation of centralized logging, preferably covering all server, endpoints and network devices. Contained is activity information with the potential to be security relevant. In most cases, these events will simply document normal IT operations: mail being sent and received, people logging in, editing documents, browsing the web, automated systems talking to each other, programs being run, clients connecting to VPNs, and so on.

   The amount of data flowing towards the SIEM can be huge, millions of events per day even for a small organization. Most of it will be completely harmless from the security point of view, and documenting the day-to-day IT operation. On the other hand, it can be very sensitive in terms of privacy implications: it contains browsing history, mail flows, names of files opened, working hours, etc.

2. In the case where the device generating the event has built in security awareness or has been fed with CTI, it can elevate a harmless event into a raw alert. Examples: the web proxy sees a connection to a known malicious domain. Multiple login failures. User runs a program from an unusual location. The EDR detects a malicious behaviour.

3. The information in the SOC's Cyber Threat Intelligence database can be used to significantly strengthen the security posture of the protected organization. On the protective side, the CTI can tell security devices what kind of activities it needs to block. These range from malicious domains that get blocked on the DNS or proxy level, known command & control hosts of adversaries, down to execution patterns that an EDR can detect and prevent.
   In other cases, the CTI data feeds into the built-in detection capabilities of devices, which can upgrade events to alerts. A good CTI database not only contains raw indicators of compromise (IOCs), but also associated use cases, playbooks, SOAR workflows and complex detection rules in standards like YARA or Sigma.

4. In a similar fashion, the SIEM relies on threat intelligence to find the traces of potentially malicious activities in the huge amount of benign events it also receives. This "operationalizing" of CTI by converting it into detection rules in the SIEM is a core competency of a successful SOC.

5. If the SIEM triggers an alert, humans have to respond and investigate. A percentage of these alerts will turn out to be false positives, which might cause the analysts to fine-tune the SIEM's ruleset. Other will be true positives, triggering the incident handling capability of the SOC.

The core function of a SOC is detection. For this purpose, it needs access to the raw, unfiltered event flow from its client and sources of CTI. It might then share the curated CTI it generates from the detected incidents with peers, but it will never share the raw data from its client.

Note that this is the simplified version of a SOC. New approaches try to integrate detection, prevention and automatic response into a unified Security orchestration, automation and response (SOAR) platform.

The European Cyber Shield

Following its introduction in a speech from Commissioner Breton on 5 April 2023, the EU commission published its proposal for the Cyber Solidarity Act on 18 April 2023. It aims to codify a number of existing initiatives into permanent law, including the European Cyber Shield[5]. In Breton's words: "We have already started with a pilot project that already brings together 17 countries in 3 large SOCs and will be deployed this year, even before the Act is negotiated."

From the EC webpage:

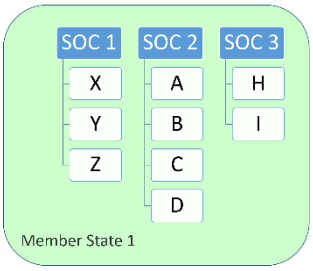
> The European Cyber Shield will be composed of Security Operations Centres (SOCs) across the EU, brought together in several multi-country SOC platforms, built with support from the Digital Europe Programme (DEP) to supplement national funding. The Cyber Shield will be tasked with improving the detection, analysis and response to cyber threats. These SOCs will use advanced technology such as Artificial Intelligence (AI) and data analytics to detect and share warnings on such threats with authorities across borders. They will allow for a more timely and efficient response to major threats. During a first phase, launched in November 2022, three consortia of cross-border Security Operations Centres (SOCs) were selected, bringing together public bodies from 17 Member States and Iceland, under the Digital Europe Programme.

The basic idea of improving the effectiveness of existing SOCs by boosting their collaboration and data sharing (both nationally and cross-border), combined with funding for CTI feeds and advanced detection technology is sound.

Visualization

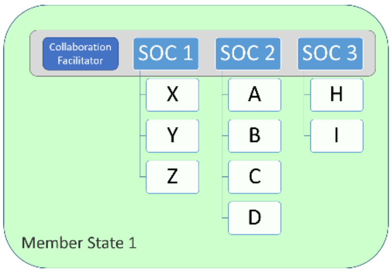
The text of the proposed Act is not easy to read. The following paragraphs with diagrams try to visualize the concept.

We start with the situation inside a single EU Member State: there are multiple SOCs that are tasked with the detection of, and response to security incidents in multiple companies. A company-internal SOC is a special case, in other instances one commercial SOC operator will act as the Managed Security Service Provider (MSSP) for multiple clients. Graphically, this looks like this (e.g. SOC 1 covers organizations X, Y and Z):



The first idea of Chapter 2 of the Cyber Solidarity Act is that these SOCs should cooperate. Instead of each buying Cyber Threat Information independently from each other and working in isolation, they should work together to improve the overall detection and reaction capability. In order to facilitate this collaboration, the EU Commission envisions a national entity that is tasked with pulling all those individual SOCs into a cooperation network. Graphically:

[5] The Cyber Defence Policy of Nov 2022 also mentions the multi-country SOC platforms that are funded via the DEP Call Digital-ECCC-2022-CYBER-03



This is eminently sensible. All those SOCs have similar tasks, they all need CTI and situational awareness to improve their detection capabilities and a close cooperation can be of real benefit. Usually, such platforms do not only focus on the purely technical exchange of data, but also try to build social interaction between the participating SOCs. Analysts can talk about recent experiences, tools and can use the colleagues in the network as a pool of knowledge.

Running such a national SOC platform comprises both providing the technical basis for the collaboration (e.g. a directory, a CTI platform like MISP, an instant messaging service, mailing lists) as well as the community management aspects (e.g. on-boarding, participation rules, meeting organization, conflict resolution, expectation management, sharing incentives, …). Some of the SOCs involved may well be competitors in the MSSP market, thus such platforms are delicate to set up correctly and run effectively. In some cases, a shared procurement of CTI feeds might be possible.

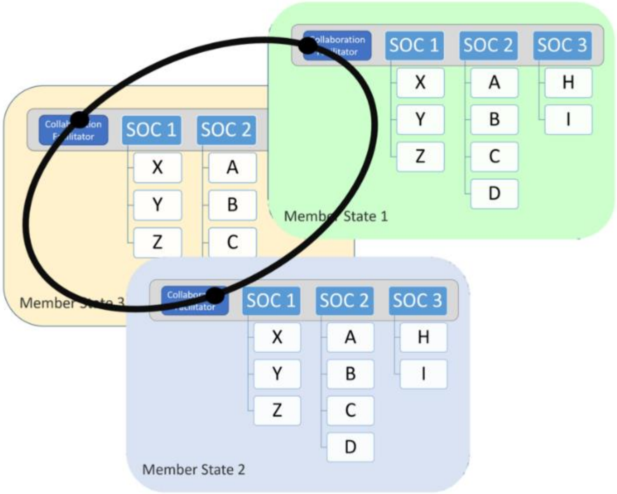
It is important to note that the facilitator as the central node in the information sharing between the SOCs does not receive the raw data (central logging, EDR information, event logs, etc.) from all the organizations protected by the SOCs. The detection of incidents still needs to happen at the individual SOCs themselves. Their automated systems (SIEMs) and the human analysts might utilize systems and data provided by the facilitator to each SOC for detection and triage purposes.

Examples of such setups are the Spanish national SOC network, national sharing portals, and various national CSIRT associations[6].

Going back the definitions of CSIRT, SOC and ISAC we find that such a national SOC collaboration forum and its facilitator is a perfect example of an ISAC: the focus is information sharing so that the individual SOCs can perform their tasks (prevention, detection and response) better.

The next step in the Cyber Solidarity Act is the collaboration between member-states. Visually:

[6] For example, see https://www.redecsirt.pt/#servicos "With a view to better understanding observed trends or malicious activity and, consequently, better preparation of preventive measures, the CSIRTs are committed to sharing indicators and statistics related to computer security problems that are likely to be distributed." [machine translation]; Various German collaboration forums also use MISP to exchange IOCs.



Member states collaborate by linking up their national SOC platforms, using the national facilitators as bridges between the national and the cross-border layer. This is a non-trivial exercise as this crosses language barriers; information needs extra context and may face legal constraints which might be resolved with an anonymization step.

There are multiple ways to set up such a "platform of SOC platforms". One can try to bring in all the individual SOCs into a big platform, or one can channel all communication via the national hubs.

Just as in the national space, the actual detection of incidents stays down at the level of the individual SOCs. The job of the cross-border network is – just as on the national level – to share CTI, situational awareness, tools and experience.

Recommendations

The concept of the Cyber Shield is sensible. Still, in order to improve the proposal, the following issues in the Commission's draft should be addressed.

Terminology

The draft Act defines the role of the facilitator of the national SOC collaboration in the following way (Article 4):

> 1. In order to participate in the European Cyber Shield, each Member State shall designate at least one National SOC. The National SOC shall be a public body.
>
> It shall have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC. It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.

First, the name is misleading. The detection still needs to happen at the individual SOC level. This national body will not have access to the raw event flow from the customers of all SOCs, thus it cannot perform the incident detection function. **Thus** (unless it also functions as the detection team of some government networks) **it does not act as a SOC itself**. It only can help the SOCs to get better at protecting their respective customers. A better choice would be "National SOC platform", or alternatively "National SOC Hub" or "National SOC Coordinator".

Secord, the sentence “It shall be equipped with state-of-the-art technologies capable of detecting, aggregating, and analysing data relevant to cybersecurity threats and incidents.” is too generic. “Detecting threats” can mean just reading Twitter. Aggregation and analysis of data on threats and incidents is something that national CSIRTs already perform. “Detecting […] Incidents” could be read as really acting as SOC, which is not realistic. A better sentence would be: “It shall support the local SOC operators by fostering collaboration and helping them to deploy state-of-the-art technologies to improve their incident detection capability.”

The “Cross-Border SOC” is defined in Article 2:

> **‘Cross-border Security Operations Centre’ (“Cross-border SOC”)** means a multi-country platform, that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment;

Again, the text calls something a SOC that is not really a SOC. As the definition says, it is “a platform” and “a coordinated network structure”. This platform will not detect incidents by monitoring some client’s network. It is a networking and support structure that will – mediated by the national coordinators – help the actual SOCs in the member states perform their function. Leaving out the word “platform” in the name is misleading, the text would be a lot clearer if “Cross-border SOC platform” would be used instead.

Yes, changing the terminology has some costs (press releases, various other policy papers, DEP call texts, …), but the cost of creating incompatible terminology is also real. The earlier this issue is fixed, the smaller the pain will be.

Relation to existing structures

The Cyber Solidarity Act is not the first EU regulation in the cyber security space. It is thus essential that the proposed new functions and structures fit into the existing ones without causing duplication.

Recital 15 states of the draft Act states:

> At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.

This is a bit of hand waving. From the NIS 2 Directive (abbreviated)

> (Article 11) The CSIRTs shall have the following tasks:
>
> - (a) monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, **providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems**;

- (b) providing early warnings, alerts, announcements and dissemination of information to essential and important entities […] on cyber threats, vulnerabilities and incidents, if possible in near real-time; […]
- (d) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;

(Article 15) The CSIRTs network shall have the following tasks:

- to exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities; […]
- to cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) in order to improve common situational awareness on incidents and cyber threats across the Union;

There is a clear overlap with the existing job descriptions of both individual national CSIRTs and the CSIRTs network. Article 11 (a) basically states that CSIRTs must be able to help the SOCs of essential and important entities to do their job on the national level, and Article 15 already specifies that the CSIRTs need to engage in cross-border CTI sharing.

The experience of 2023 with the three consortiums entering the CfEI / DEP call for "cross-border SOC platforms" shows quite clearly that all the entries involved in these proposals are also members of the CSIRTs network (except for Austria, where CERT.at was blocked from direct participation via the "public body" requirement).

How can this be resolved?

On the national level, it makes sense to use the same language and process as Article 12 NIS2 where the role of the national coordinating CSIRT for the purpose of CVD is defined like this:

> Each Member State shall designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure.

The Cyber Solidarity Act could use text like (modelled after Article 12 NIS2)

> Each Member State shall designate at least one of its CSIRTs as a coordinator for national SOC collaboration ("national SOC coordinator") and as the bridge to the European Cyber Shield.

or (modelled after Article 10 NIS2)

> Each Member State shall designate or stablish one national SOC platform. A SOC platform may be designated within one of the CSIRT stipulated in Art 10 EU2022/2555.

On the EU level, the long-term vision needs to be that detailed information about threats suitable for SOCs is shared between the "national SOC platforms" in all member states.

The Commission wisely decided against creating a full "SOCs network" in parallel to the CSIRTs network, and opted to start with smaller groups instead[7]. This is the really good idea of Chapter 2 of the Cyber Solidarity Act: the notion that the EU will co-fund projects of groups of member states that commit to a closer collaboration, including shared infrastructure and procurement, than what is

[7] See also https://cert.at/en/blog/2023/7/a-network-of-socs for arguments on why starting with small groups makes sense

currently done (and feasible[8]) in the context of the CSIRTs network. The pilot projects[9] from the 2022 DEP call make a lot of sense, as they will develop technology, structures and processes for effective cross-border collaboration.

Adding participants to these cross-border collaboration platforms and linking them up is already foreseen in the text (Articles 4 and 6).

Chapter 2 of the Cyber Solidarity Act is necessary to fund this expansion of the cross-border SOC collaboration projects that are starting up now.

What is missing is a clear definition of the relationship to the CSIRTs network, especially with the future in mind where these small cross-border platforms have grown to cover all EU member states. While it is hard to predict how this will develop exactly, Metcalfe's law, combined with the friction of data-exchange between cross-border platforms, suggests that in the end, there might be only one to two such platforms.

One possible conclusion is that the cross-border platforms start as subsets of the CNW, which over time may grow to cover the full network.

This also resolves Article 7 of the proposed act, which deals with interactions with other EU entities. There is an established process how information from a CSIRTs Network member about an incident flows both nationally to their CyCLONe participant, as well as on EU level to the full CSIRTs Network and even the relevant SPOCs. There is no need for Article 7 to define additional information flows, let alone allow implementing acts for these.

Conclusions

The EU Cyber Shield is a helpful and welcome initiative.

The terminology used should be improved as it causes misunderstanding.

A clarification regarding the relation of the Cyber Shield with existing CSIRTs and the CSIRTs network would also be welcomed.

[8] Cross-border information sharing cannot be at a higher level of maturity than how it is done nationally. There is a lot of variation in the CSIRTs Network members' capabilities. And as mentioned above, the joint procurement option is not possible with all CSIRTs Network members.

[9] „We have already started with a pilot project that already brings together 17 countries in 3 large SOCs and will be deployed this year, even before the Act is negotiated." Breton, 5 April 2023