Booklets on National Cybersecurity Institutions

Dr. Tadas Jakštas

DCAF Geneva Centre for Security Sector Governance

Table of Contents

Booklets on National Cybersecurity Institutions

Introduction

DCAF's project, 'Good Governance in Cybersecurity in the Western Balkans', supported by the United Kingdom's Foreign, Commonwealth and Development Office, includes building the institutional cybersecurity capacity of six economies: Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia. Towards this objective, three booklets with tangible guidelines have been developed:

- Setting Up National Cybersecurity Agencies
- Setting Up and Regulating Sectoral CERTs
- Strengthening Cooperation with Private Sector Actors for Networking and Information Sharing

Within the frame of seminars and conferences that bring together regional stakeholders, these three booklets have been developed following a Regional Seminar on Best Practices in Cybersecurity Legislation, which was held in Slovenia in March 2022. Accordingly, they take into account the bottom-up feedback received from experts and participants.

Taken together, these booklets provide tangible frameworks and insights for public and private sector stakeholders who lead key institutions that underpin a country's cybersecurity institutional architecture. They help build bridge not only among the main stakeholders, but also the continuum from legislation into regulation, and institutional development and cooperation.

About the author

Dr. Tadas Jakštas is a senior consultant on cybersecurity capacity building who has managed international and national projects. Currently, Dr. Jakštas works at NRD Cyber Security, a technology consulting, incident response and applied research company, where he is responsible for leading multi-stakeholder cyber security capacity building, especially in the areas of strategy, legislative frameworks, critical information infrastructure, and governmental and sectorial CSIRTs. Dr. Jakštas led the maturity assessment project, extended the framework beyond CSIRTs Network in cooperation with ENISA, and has implemented capacity building projects in Qatar, Serbia, Ecuador, Rwanda and Lithuania. He is also a trainer of SECO Institute - Crisis Management Foundation course.

Prior to joining NRD Cyber Security, Dr. Jakstas worked at the NATO Energy Security Centre of Excellence, where he was responsible for projects related to critical information infrastructure protection, crisis management and industry systems cybersecurity.

Setting Up National Cybersecurity Agencies

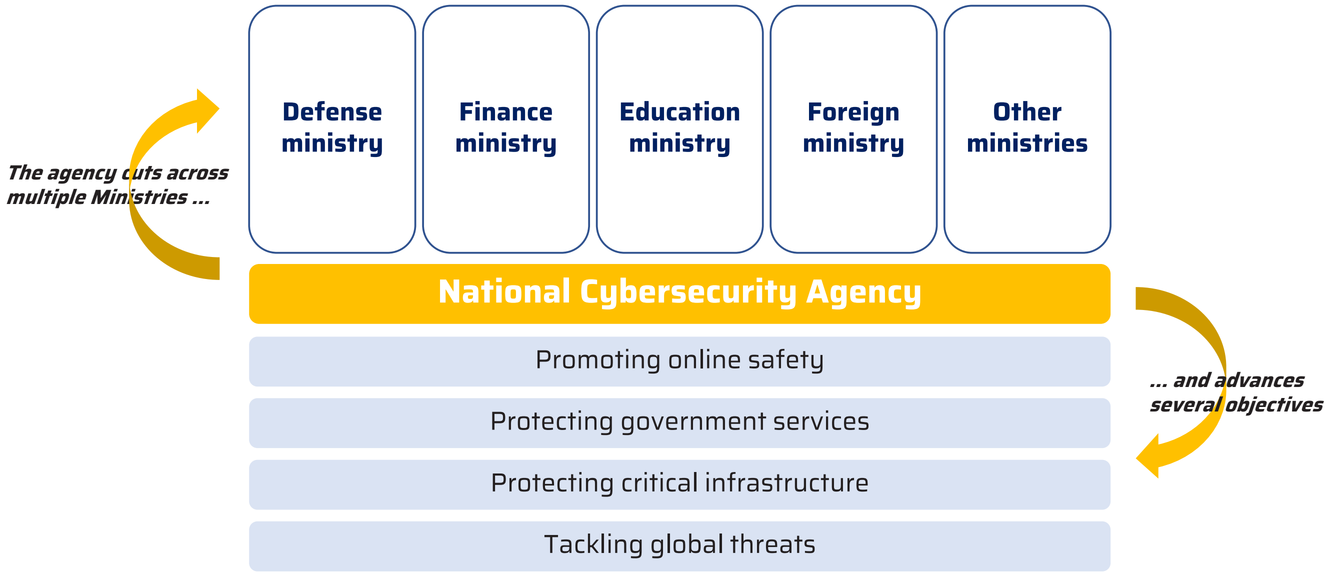
DCAF Geneva Centre for Security Sector Governance

Introduction

Information and communication technology (ICT) is now a firmly established pillar of modern life. Continuous and rapid innovation has resulted in a profound digital transformation of social, economic, and government frameworks. It has brought numerous benefits, from increased effectiveness and productivity to easier access to information and learning. It has also, however, exposed increasing numbers of individuals, businesses, and governments to new threats.

To reap the benefits of digitalization while effectively responding to cyber threats, many governments are currently working to adopt, review, or implement national cybersecurity strategies, policies, laws, and regulations – or other national approaches – with countless other efforts taking place at the sectoral, state, city, or other level. Certain countries have considered establishing a central cybersecurity agency or a similar body to support the development of a cybersecurity ecosystem and to help manage their cybersecurity priorities.

The task of such agencies is nevertheless complex, not only because of the pervasiveness of computing today, but also because of the legacy of pre-digital era policymaking and regulations. Cybersecurity is one of the first policy areas to challenge traditional governance structures and policymaking. National cybersecurity approaches must tackle a great deal, from promoting online safety and protecting government services and critical infrastructure (CI), to engaging internationally to tackle global threats. These topics cut across an unprecedented range of traditional government departments, from defence and foreign affairs to education and finance.



The agency cuts across multiple Ministries ...

Defense ministry

Finance ministry

Education ministry

Foreign ministry

Other ministries

National Cybersecurity Agency

Promoting online safety

Protecting government services

Protecting critical infrastructure

Tackling global threats

... and advances several objectives

I. Benefits of establishing a cybersecurity agency

The benefits of establishing a cybersecurity agency include:

- the coordinated management of national cybersecurity priorities;
- a pool of national cybersecurity expertise under one roof;
- effective and broad communication with national cybersecurity stakeholders; and
- established clear roles and responsibilities for managing a cybersecurity ecosystem.

II. Challenges of setting up a cybersecurity agency

The challenges of establishing a cybersecurity agency include:

- unclear objectives and responsibilities for the agency;
- a lack of leadership support;
- a siloed mindset that prevents the effective governance of the cybersecurity ecosystem; and
- a lack of engagement from the public and private sector.

III. Recommendations for setting up a cybersecurity agency

Recommendations for establishing a cybersecurity agency include the following:

1. Appoint a single national cybersecurity agency:

Setting up a single agency dedicated to managing cybersecurity at the national level can be an effective means of managing the security of civilian agencies, CI protection, and national-level incident response. Governments have limited time, expertise, and resources to deal with the range of threats they face. Integrating core national-level functions related to coordination, standards setting, incident response, partnership, and international outreach into one agency will allow governments to prioritize their limited resources. In addition, having a single agency that facilitates such coordination also ensures that agencies do not duplicate efforts. Some governments may choose to continue to distribute expertise across government agencies but identify a single body responsible for oversight and establish a clear coordination process – in essence a virtual agency to increase accountability and unify efforts.

2. Ensure a clear mandate for the national cybersecurity agency:

A national cybersecurity agency will be expected to navigate a complex environment that spans other government departments, national legislatures, established regulatory authorities, civil society groups, the general public, public and private sector organizations, and international partners. It is therefore important that all stakeholders are familiar with the mandate of the national cybersecurity agency to ensure they have clear expectations and know who the primary points of contact are.

It is also critical that the roles and responsibilities of the national cybersecurity agency are different from those of other governmental stakeholders involved in cybersecurity (for example, regulators in CI sectors – including energy, transport, and financial services – that, in some contexts, develop security policies relevant to their industry).

3. Ensure the national cybersecurity agency has appropriate statutory powers:

Currently, most national cybersecurity agencies are established not by statute but by delegating existing powers from other parts of government. This is consistent with the current approach taken in most other jurisdictions with a national cybersecurity agency.

Nevertheless, this approach is expected to change as more and more governments pass comprehensive cybersecurity laws. The enforcement of these laws may require the establishment of specific cybersecurity bodies, such as a national cybersecurity agency.

The following internationally agreed cybersecurity principles could be used to guide statutory measures to establish a national cybersecurity agency:

- **Risk-based approach:** The agency should seek to manage the cybersecurity environment through a proportionate, risk-based framework that enables organizations to innovate and adopt new technologies without exposing the country to unnecessary cybersecurity risks.

- **Outcome-focused approach:** It is essential that the agency focuses on delivering the desired end state, rather than prescribing the means to achieve it, and then measures progress towards that end state.

- **Prioritization:** Not all threats are equal. The national cybersecurity agency should adopt a graduated approach to criticality, prioritizing CI risks.

- **Practicable and realistic:** Cybersecurity policies are of little value if they impose undue burdens on the organizations that must comply with them. Engagement with industry is a necessary first step to ensuring that policies are practicable and realistic.

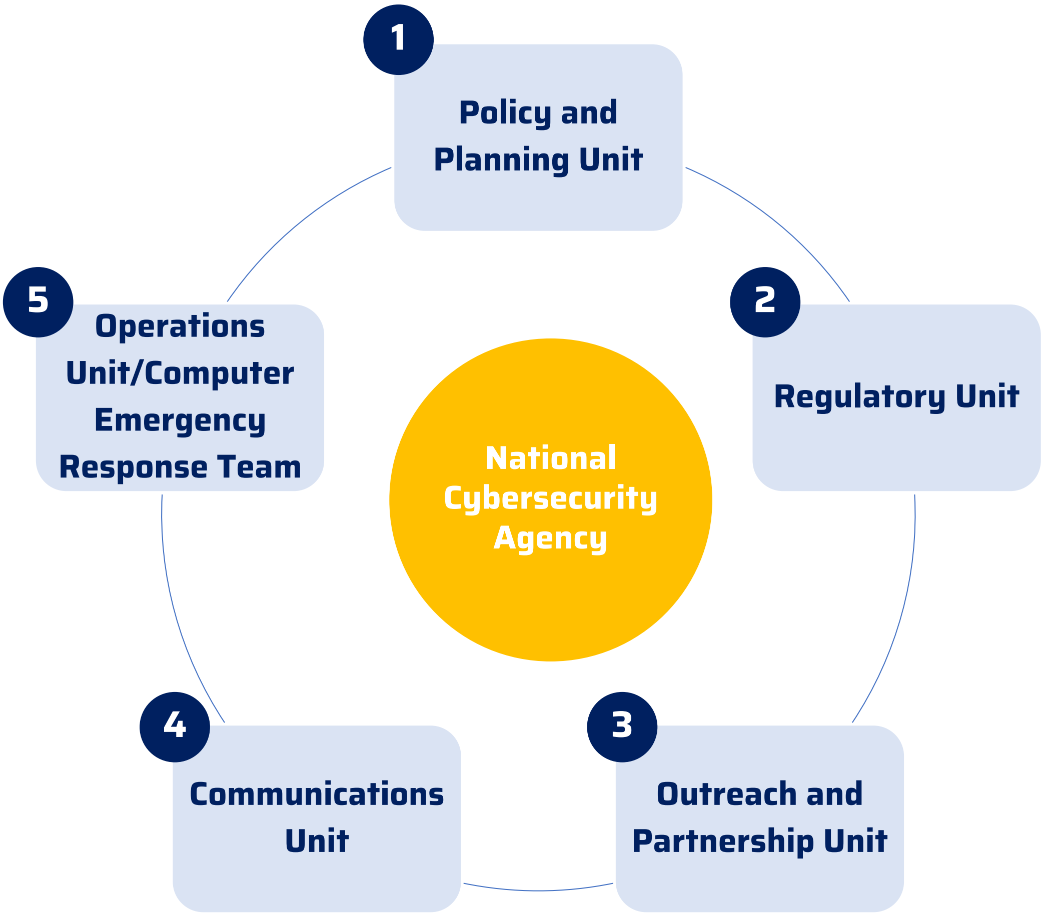
- **Human rights and fundamental values:** Enforcing cyberspace principles cannot come at the cost of sacrificing privacy, civil liberties, and the rule of law. Instead, a balanced approach is needed that respects these fundamental principles.

- **Globally relevant:** The national cybersecurity agency should leverage international standards to the greatest extent possible. Cybersecurity is a problem that transcends territorial boundaries; it is therefore important that the country does not take steps that may limit its ability to collaborate with international partners.

4. Ensure the national cybersecurity agency has a clear organizational and governance structure:

Based on best international practices, the national cybersecurity agency could be composed of five components, as outlined below, each with a specific mandate but working in collaboration with the others:

- ❖ a policy and planning unit;
- ❖ a regulatory unit;
- ❖ an outreach and partnership unit;
- ❖ a communications unit; and
- ❖ an operations unit/computer emergency response team (CERT).


1
Policy and Planning Unit
2
Regulatory Unit
3
Outreach and Partnership Unit
4
Communications Unit
5
Operations Unit/Computer Emergency Response Team
National Cybersecurity Agency

This five-part structure allows for a multifaceted interaction between internal government and regulatory stakeholders and external stakeholders from the public and private sectors, as well as the international arena. In particular, it addresses one of the core challenges governments face in establishing national cybersecurity agencies: how to reconcile mandatory reporting of cyber incidents, handled by the regulatory unit, with the voluntary and two-way exchange of information about cyber threats and cyber incidents, handled by the CERT. The structure achieves this by placing the regulatory unit and the CERT within the same framework and then developing policies to control the flow of data between the two.

5. Ensure the national cybersecurity agency has adequate capacities and capabilities to evolve and adapt over time:

Due to the rapid evolution of ICT and constantly evolving regional and international standards and baselines around cybersecurity, from risk management through to resilience, it is inevitable that the national agency will need to evolve and adapt over time if it is to continue to fulfil its mandate.

For any national cybersecurity agency such developments could include modifying the mandate, acquiring staff with new skills, developing new partnerships with public and private sectors or international organizations, and so on. In such a dynamic and evolving environment, a national cybersecurity agency must be able to make the necessary adjustments to its structure and operations and have the authority to be listened to by policymakers or legislators when requesting that those changes be made.

IV. Examples of established cybersecurity agencies

National Cybersecurity Centre of Lithuania

The National Cyber Security Centre (NCSC), under the Ministry of National Defence, is the main Lithuanian cybersecurity institution. It is responsible for coordinating the management of cyber incidents, monitoring and controlling the implementation of cyber security requirements, and allocating information resources.

The NCSC's mission is to be the centre of cybersecurity expertise for effective cybersecurity incidents and to provide a strong cyber security prevention system in the country. Regulations approved by the NCSC provide for the following main operational goals of the institution: to implement a national cyber security policy; to perform the functions of the security service and the national communications protection service; and to disseminate information and undertake research and analysis on cybersecurity issues. Since 2018, the one-stop-shop principle of the NSCS enables assistance to be provided to the state, as well as to businesses, institutions, and residents. Within the limits of its competence, the NCSC makes decisions – along with state institutions, organizations, and other economic entities – on issues related to state information resources, critical information infrastructure, and cybersecurity.

The NCSC was established after the Law on Cybersecurity of the Republic of Lithuania entered into force on 1 January

2015, which established the legal basis and consolidated joint efforts to protect Lithuanian cyberspace.

National Cyber Security Centre in the UK

Launched in October 2016, the National Cyber Security Centre (NCSC) has its headquarters in London and brings together expertise from its National Technical Authority for Information Assurance (known as CESG)—the information assurance arm of Government Communications Headquarters (GCHQ)—the Centre for Cyber Assessment, CERT-UK, and the Centre for the Protection of National Infrastructure.

The NCSC provides a single point of contact for small and medium-sized enterprises, larger organizations, government agencies and the general public. It also works collaboratively with other law enforcement and defence agencies, the UK's intelligence and security agencies, and international partners.

More specifically, the NCSC:

understands cybersecurity, and distils this knowledge into practical guidance that is made available to all;

responds to cyber security incidents to reduce the harm they cause to organizations and the UK;

uses industry and academic expertise to nurture the UK's cybersecurity capability; and

reduces risks to the UK by securing public and private sector networks.

V. References and further reading

Nicolas, Paul and Kaja Ciglic. 2017. Building an Effective National Cybersecurity Agency. Microsoft. Available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-agency-whitepaper.

National Cybersecurity Centre of Lithuania. Available at: https://www.nksc.lt/en/structure.html.

National Cyber Security Centre in the UK. Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

National Cyber Security Centre in the Netherlands. Available at: https://english.ncsc.nl/about-the-ncsc/statutory-task.

Setting Up and Regulating Sectoral CERTs

DCAF Geneva Centre for Security Sector Governance

Introduction

As governments and critical infrastructure (CI) operators incorporate more connected technologies into their systems, cybersecurity risks continue to increase. In response to these risks, many governments around the world have begun to dedicate more resources toward cybersecurity, as well as toward the protection of CI and critical sectors of their countries or economies.

Regardless of which sectors are prioritized or defined as critical by a country or economy, cybersecurity threats to CI can have devastating consequences. One of the most effective ways to counter these threats is to create a global ecosystem of computer emergency response teams (CERTs) and security operations centres (SOCs) that can share information, and respond to cyber threats effectively. This process can be facilitated by developing relevant frameworks and increasing the number of sectoral CERTs.

A sectoral CERT is fundamentally a body that supports incident response and management for a specific sector of the country or economy. In rare cases, a sectoral CERT goes further, performing central tasks and functions related to computer security incidents that occur in the sector, including the following:

- leading or facilitating incident response;
- communicating and coordinating with members of the sector and other stakeholders;
- coordinating with the national CERT and within the national cybersecurity ecosystem;
- disseminating information before and after incidents;
- convening meetings and facilitating discussions among stakeholders;
- providing or leading training; and
- ensuring trust and confidentiality among members.

I. Benefits of setting up sectoral CERTs

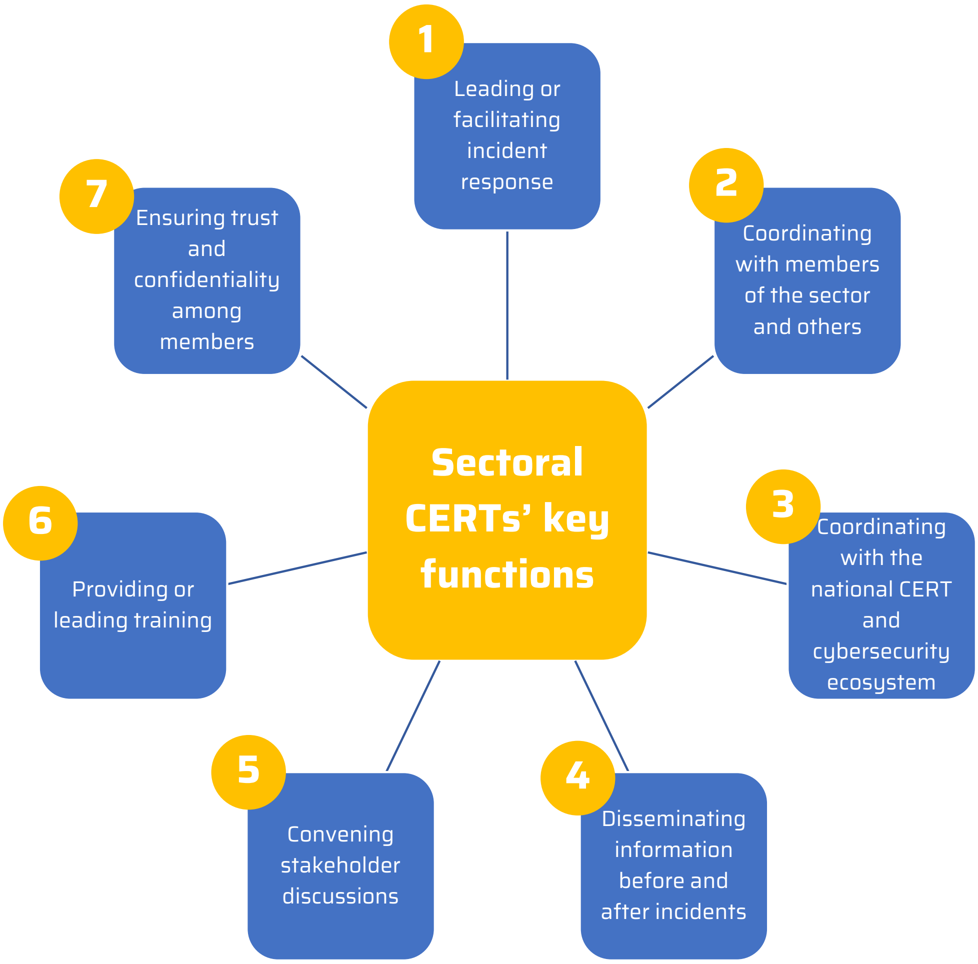
The benefits of establishing a sectoral CERT include:

- specific information and in-depth knowledge of their sector;
- a sector-specific network of contacts;
- closer relationships with vendors of the sector;
- expertise on sector-specific hardware and systems;
- sector-specific conferences, workshops, and training;
- the creation of uniform frameworks for audit documentation at the sectoral level;
- a faster sectoral communication channel, as their constituency base is smaller than that of a national CERT; and
- sector-specific recommendations.

II. Challenges of setting up sectoral CERTs

The challenges of establishing sectoral CERTs include:

- an unclear mandate, vision, or objectives for sectoral CERTs;
- a lack of leadership support;
- a lack of effective governance and legal structures;
- unsustainable financial mechanisms;
- a lack of engagement and cooperation among public and private stakeholders;
- ineffective communication with constituents and stakeholders; and
- a service model for sectoral CERTs that is not tailored to the needs of participants.


Sectoral CERTs' key functions
1
Leading or facilitating incident response
2
Coordinating with members of the sector and others
3
Coordinating with the national CERT and cybersecurity ecosystem
4
Disseminating information before and after incidents
5
Convening stakeholder discussions
6
Providing or leading training
7
Ensuring trust and confidentiality among members

III. Recommendations for setting up a sectoral CERT

The recommendations for setting up a sectoral CERT can be divided into the five categories discussed below:

1. Understand the need for a sectoral CERT:

Cybersecurity leaders in a country or economy may wish to implement a sectoral CERT if they recognize the need for an organization that offers the advantages described above or if there is a need for additional cybersecurity and incident response capacity in a particular sector. This additional capacity could take the form of increased scalability or expertise:

- **Scalability:** It can be difficult to scale a national CERT's services to the owner/operator level. A sectoral CERT responds to most of these sector-specific needs to allow the national CERT to focus on coordinating across sectors and with others in the ecosystem.

- **Expertise:** Addressing CI sector incidents can require specialized knowledge and skills. While a national CERT may not have the resources to address the specific needs of each sector, a sectoral CERT can maintain subject matter expertise relevant to its sector's needs.

To establish and implement the sectoral CERT, the development team must answer the following questions:

- Who will define the sectoral CERT, and what will that definition be?
- What legal authorities, if any, will the sectoral CERT have?
- What will the scope of the sectoral CERT's responsibilities be?
- What will the composition of the sectoral CERT be, particularly as it relates to funding, staffing, and acquiring and sharing information?

2. Understand the national cybersecurity ecosystem:

One important consideration is the degree to which the sectoral CERT will be integrated into the national cybersecurity ecosystem – that is, the collection of agencies, teams, and stakeholders that work together to protect a nation's cybersecurity and information assets. This ecosystem can include public sector entities (such as the national CERT, law enforcement, and regulatory bodies) and private sector entities (such as other sectoral CERTs, private cybersecurity companies, and academia).

The development team can include a national CERT or other components of the national cybersecurity ecosystem. These stakeholders can, however, also assume additional roles, including as sources of information, collaboration, and guidance during each part of the process. The extent of the national cybersecurity ecosystem's involvement in this process depends on the sectoral CERT's level of integration in that ecosystem. For example, a sectoral CERT that is created by law and housed within a government agency is likely to be closely integrated with the national CERT and other national partners in that ecosystem. On the other hand, a sectoral CERT that is created and operated by private sector entities (such as an industry association or a group of CI operators) may have only loose ties to the rest of the national cybersecurity ecosystem.

A national CERT is responsible for the cyber protection of a country or economy. There are many models of national CERTs; however, regardless of the model used, every national CERT has broad responsibilities and missions.

In contrast, a sectoral CERT is responsible for a smaller subset of the country or economy (that is, the particular sector it serves). In many cases, this arrangement leads to an overlap of responsibilities between the sectoral CERT and the national CERT. Successfully integrating the sectoral CERT into the national cybersecurity ecosystem therefore requires a strong working relationship between the two. In some cases, however, particularly in countries with nascent or developing cybersecurity capabilities, a national CERT may not exist.

The sectoral CERT development team should consider the following questions:

- What role will the national CERT (if one exists) play in the sector?
- What relationship will the sectoral CERT have with the national CERT (if one exists)?
- If there is no national CERT, how does this affect the sectoral CERT's role in the national cybersecurity ecosystem?
- How will the sectoral CERT address issues related to working with the public and private sectors at the national level?

The success of many aspects of a sectoral CERT's mission (such as information sharing) depends on trust – another factor that affects the cybersecurity ecosystem. The development team must therefore carefully consider how the new sectoral CERT will establish and maintain trust with a variety of stakeholders, from the prerequisite stage through to post-implementation and beyond. These stakeholders include constituents, information-sharing partners, and the national CERT.

3. Identify and define the sector:

For a proposed sectoral CERT to be established and operationalized, it must be able to define the sector it aims to support. It is important to conduct preliminary research to determine the scope and applicability of the name chosen for the sector and to understand the sectoral CERT's objectives.

The definition of each sector can vary depending on the situation or country. For example, the financial sector may be limited to banks in one country, but include other financial institutions, such as credit card companies or investment firms, in another. No single definition of a sector is appropriate for every setting; the team responsible for the development of the sectoral CERT should choose the definition that best fits its needs and situation. If the team does not identify the sector and its scope itself, it must know who will make, or has made, this decision. Besides identifying the sector that the CERT will support, the development team must also describe and define the entities included in the sector, ensuring that all relevant participants and stakeholders are accounted for. While the sector's identity describes what the sector is, this part of the process identifies the specific members of the sector.

The sectoral CERT development team must understand which organizations should be included in or consulted about the sectoral CERT, such as stakeholders, constituents, and community members:

- **Stakeholders:** A stakeholder is any organization or entity that has an interest in or is concerned with the proposed sectoral CERT. While a stakeholder may not be directly served by the sectoral CERT, it may receive significant secondary benefits.
- **Constituents:** Typically, constituents are a subset of stakeholders. While stakeholders include all organizations and entities that affect or are affected by the sectoral CERT, constituents are organizations and entities that are served by the sectoral CERT – that is, bodies that have cybersecurity and incident response services provided to them.

4. Identify a suitable entity to host the sectoral CERT:

The parent organization of a sectoral CERT is referred to as the host entity. If a sectoral CERT is a standalone entity, however, it may not have a host entity or be part of a hierarchy. Since the lack of a host entity poses challenges, the development team should consider all relevant factors when a sectoral CERT is a standalone entity. Whether determining the host entity of the sectoral CERT or considering additional factors, input is required from many stakeholders and several key issues must be taken into account.

When the development team considers where and how to host a sectoral CERT, it develops an understanding of which organizations, agencies, and other stakeholders are familiar with the current environment as it relates to (1) the sector at large, and (2) the state of cybersecurity and incident response in the sector. Entities with sector-specific knowledge are uniquely positioned to provide guidance on many aspects related to developing and operating a successful sectoral CERT. Even organizations that do not have technical or security-related knowledge can provide valuable input based on their deep historical knowledge of the sector (such as the operations, economics, and politics). For example, a banker's association may have little insight into cybersecurity and incident response, but it can provide important information about the financial sector, such as its critical assets.

In many cases, the host entity for the sectoral CERT is known or determined in advance. Legislation or a government policy or directive may dictate where a particular sectoral CERT should fall within the existing incident response hierarchy. If the development team starts to establish the sectoral CERT before a host entity is determined, it should strive to identify the host entity as soon as possible to avoid the need to revisit policies, procedures, and practices if the host determination is decided later in the process.

5. Understand legislation and legal authority or guidance:

For a sectoral CERT to be successful, it must have the legal authority to operate. This is true regardless of the exact nature and form of the sectoral CERT (such as private vs. public or large vs. small) and its mission. While the nature of legal authority varies from jurisdiction to jurisdiction, the actions that the sectoral CERT can and cannot take must be clearly defined, along with its methods of interaction with relevant government authorities and its responsibilities (such as incident reporting requirements).

Legislation often defines the sector supported by the CERT. This is a crucial component, particularly when the sectoral CERT is a public or government-run body or when it supports CI since its authority can be defined in a law or another legally binding policy. The development team must in any case understand the legal and legislative environment in which the sectoral CERT is established and operates.

It should be emphasized that legal authority does not always come in the form of a legislative edict. Executive orders, agency or ministry rules and regulations, and other official and binding policy directives should be examined as part of the legal landscape in which the sectoral CERT will reside. This type of legal guidance establishes the limits and requirements that the sectoral CERT must adhere to.

In addition to existing laws, policies, and other regulations, other factors, detailed below, can also be relevant to establishing a sectoral CERT and should be considered by the sectoral CERT development team. Understanding the following factors from the start of the sectoral CERT development process can mitigate unforeseen challenges:

What is the level of authority mandated by existing legislation or regulations? Legal environments can be complicated. Statutory compliance (that is, compliance with laws) is different from regulatory compliance (that is, compliance with rules). Security laws can differ from privacy laws. Legal requirements have different implications than legal guidelines. Understanding the level of authority and type of compliance required is an important part of setting the groundwork for an effective, functional sectoral CERT.

Is legislation drafted but not implemented? Establishing a sectoral CERT under one legal framework only to see that legal framework significantly change shortly before or after sectoral CERT operations begin can lead to duplicated efforts. The development team should know whether significant legal changes are expected in the short term, and consider waiting to proceed until these changes become official.

Is legislation or regulation enforced? Regulations and legal edicts may not be enforced for many reasons (such as political issues, lack of interest or capacity on the part of law enforcement, and court rulings). Understanding whether, and if so why, laws and regulations are not enforced leads to better decision-making processes about how to position the sectoral CERT.

- ✓ **Understand the need for a sectoral CERT**
- ✓ **Understand the national cybersecurity ecosystem**
- ✓ **Identify and define the sector**
- ✓ **Identify a suitable entity to host the sectoral CERT the capability**
- ✓ **Understand legislation and legal authority or guidance**

IV. Examples of established sectoral CERTs

CERTFin (Italy)

The CERTFin was created through a special agreement between the Italian Banking Association, the Bank of Italy, and ABI Lab signed on 20 December 2016.

CERTFin is the focal point for the collection, analysis, and sharing of information related to cyber threats, and for the coordination of activities to prevent and support response to cyber emergencies that could harm IT assets of the Italian financial and insurance organizations participating in the constituency.

The CERTFin's constituency comprises financial and insurance organizations that adhere to CERTFin.

The main goals of CERTFin are:

- to provide prompt information regarding potential cyber threats that could damage banks and insurance organizations;
- to act as point of contact between financial operators and other relevant public institutions on issues related to cyber protection;
- to facilitate the response to large-scale security incidents;
- to support the crisis management process in the event of cyber incidents;
- to cooperate with national and international institutions and other actors, from both the public and private sector, that are involved in cyber security, by promoting the cooperation among them; and
- to improve cybersecurity awareness and culture.

Creation of the Z-CERT (The Netherlands)

The Z-CERT was founded in 2017 by a group of Dutch hospitals to help healthcare institutions with cybersecurity protection and incident support. In 2017, all Dutch hospitals were found to have vulnerabilities in their systems. The most prominent risks were configuration errors and websites running on outdated software. The Z-CERT was established to overcome these IR weaknesses and provide specialized incident response services to healthcare institutions. The Z-CERT and National Cyber Security Centre (NCSC) work together by sharing relevant information and data.

Today, all hospitals (including academic 'UMCs', top clinical 'STZ', and 'general' hospitals) and mental healthcare institutions ('GGZ') can register with Z-CERT as participants of the Health Sectoral CERT constituency, and can therefore benefit from Z-CERT cybersecurity protection and incident response support and knowledge.

It appears that the responsibilities and services of the Z-CERT will soon be expanded. COVID-19-related developments have accelerated the Z-CERT's plans to implement cyber threat intelligence capability as well as other projects to enhance the digital resilience of the Dutch healthcare system.

V. References and further reading

ENISA (European Union Agency for Cybersecurity). 2021. CSIRT Capabilities in Healthcare Sector. Available at: https://www.enisa.europa.eu/publications/csirt-capabilities-in-healthcare-sector.

ENISA. 2020. How to set up CSIRT and SOC. Available at: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

ENISA. 2020. Sectoral CSIRT Capabilities: Energy and Air Transport. Available at: https://www.enisa.europa.eu/publications/sectoral-csirt-capabilities-energy-and-air-transport.

Novak, J., et al. 2021. The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities. Carnegie Mellon University. Available at: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf.

Strengthening Cooperation with Private Sector Actors for Networking and Information Sharing

DCAF Geneva Centre for Security Sector Governance

Introduction

Building strong, trusted networks between critical information infrastructure protection (CIIP) stakeholders and enabling the sharing of information both play an important role in safeguarding society. The timely and speedy sharing of cybersecurity-related information between critical information infrastructure (CII) stakeholders – within the government and critical sectors, across sectors, between public and private organizations, and both nationally and internationally – is widely perceived to be an effective measure to address some of the cybersecurity challenges of CII operators.

Information sharing, in this context, usually involves a group of carefully chosen people with a mutual goal: to keep abreast of new and emerging threats and vulnerabilities, and related issues. It is important to choose those with a similar level of technical knowledge, authority and autonomy, and risk appetite. These individuals share information in order to be able to take appropriate risk-mitigating measures, not only before and during incidents but also in their aftermath. They meet regularly, develop personal trust, and share sensitive information about incidents, threats, vulnerabilities, good practices, and solutions. They typically do this in a confidential environment where they undertake not to disclose the details or to use the information to protect their own systems. There are many variations on this model, as discussed below.

There are two key factors for successful information exchange: trust and value. To initiate and maintain the sharing of knowledge and information, CIIP stakeholders need to work in an environment where trust can be established and sustained in an efficient and effective way. The physical environment may influence the experience of and attitude towards the information exchange. The ‘environment’ may also be influenced by how the exchange takes place (such as through regular, regulated, formal, or informal rules) and how previous efforts of public bodies were received by relevant stakeholders. Establishing an environment of trust and value requires time and commitment from all participants. The added value of improved and trusted information, however, far outweighs this investment.

In practical terms, fostering relations with other public organizations, as well as with private organizations, may involve different approaches. In many countries, the majority of CI and CII is operated by private organizations. Government intervention can take place in the form of collaborative agreements between public and private sectors. If a country’s CII is mostly operated by private entities, the government can support information sharing, facilitate and stimulate cooperation, and perform control and oversight through legal and regulatory instruments. Public-private partnerships (PPPs) are often employed to provide a framework for the relationships between government and private operators. Such partnerships can reduce risks and lower costs for the organizations involved because of improved collaboration. It is important, however, that the actors involved advocate clear roles and responsibilities, irrespective of the chosen approach to structuring stakeholder relations.

I. Benefits of strengthening cooperation with private sector actors

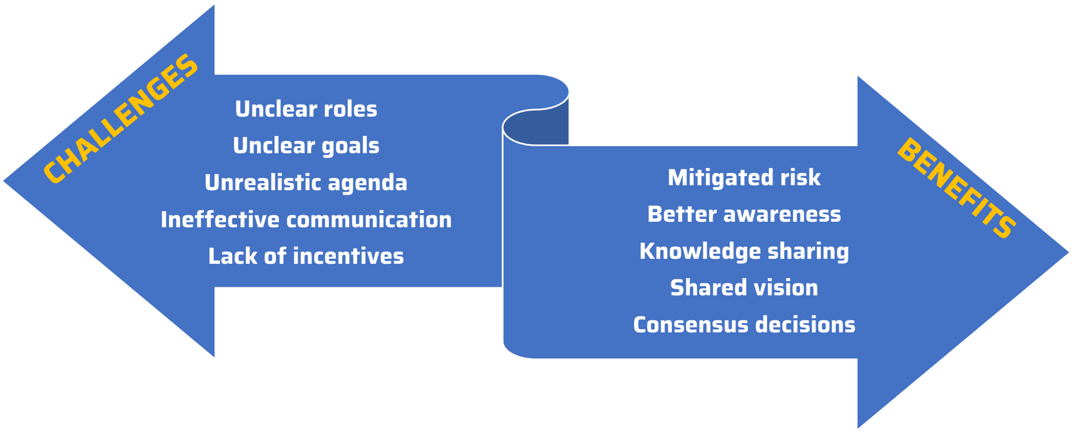
The benefits of strengthening cooperation with private sector actors include:

- improved management and mitigation of cybersecurity risks at the operational level;
- a better overview and situational awareness of potential threats and vulnerabilities, and their impact on the organization;
- the ability to leverage knowledge, awareness, understanding, and experiences across a broader community;
- the opportunity to develop a shared vision on CII resilience; and
- the opportunity to build consensus on strategic decisions regarding CIIP.

II. Challenges of strengthening cooperation with private sector actors

The challenges of strengthening cooperation with private sector actors include:

- unclear roles and responsibilities for cooperation;
- a lack of clear objectives for cooperation;
- an overly ambitious and unrealistic agenda for cooperation;
- ineffective communication with and outreach to the private sector; and
- a lack of incentives for the involvement of the private sector.



III. Recommendations for strengthening cooperation with private sector actors

Recommendations for strengthening cooperation with private sector actors include the following:

1. Encourage the sharing of cybersecurity-related information:

Information sharing provides a basis for the common understanding of threats, vulnerabilities, and dependencies, and shared knowledge on possible countermeasures. Information sharing improves the quality of risk management because information on new risk factors may be available more quickly. The CII protection measures may be adapted accordingly. When major CII disruption occurs, the existence of a trusted network with common interests and experiences helps to address the incident effectively and collaboratively. Information sharing is therefore an effective approach to help manage the collaborative CII risk in a domain where the threat landscape is changing continuously. Experiences of successful voluntary information-sharing initiatives show that trust is a key factor to success. An agreement that defines how each organization may use the information exchanged supports these efforts. In many nations, the Traffic Light Protocol (TLP) is a proven way to enable information sharing between private and public organizations. Information sharing, however, is a multifaceted notion with many related policy issues, both from the public and the private side.

2. Establish clear roles in CIIP information-sharing initiatives:

There are examples of good practices around the world where stakeholders in CIP/CIIP are involved in information-sharing initiatives at a regional, national, or international level. Some of these initiatives are government to government (G2G) or business to business (B2B), but many public-private initiatives are also in place. Examples include the Forum for Incident Response and Security Teams (FIRST); the European Government CERTs (EGC) group; InfraGard; several information sharing and analysis centres (ISACs) in the EU and US; the UK's Cyber Security Information Sharing Partnership (CiSP); the German UP KRITIS; the UK's Centre for the Protection of National Infrastructure (CPNI) information exchanges; the Reporting and Analysis Centre for Information Assurance (MELANI) in Switzerland; and the NCSC's ISAC in the Netherlands. In many of these initiatives, CIIP stakeholders come together and actively share information about threats, incidents, vulnerabilities, and good practices.

3. Establish cyber threat information-sharing initiatives:

Cyber threat information is any information that can help an organization identify, assess, monitor, or respond to cyber threats. It includes indicators of compromise; tactics, techniques, and procedures used by threat actors; recommended actions to detect, contain, or prevent attacks; and findings from the analyses of incidents. Organizations that share cyber threat information can improve their own security postures as well as those of other organizations.

The 'References and further reading' section provide guidelines for establishing and participating in cyber threat information-sharing partnerships. This guidance helps organizations to establish information-sharing goals, identify cyber threat information sources, assess information-sharing activities, develop rules that control the publication and distribution of threat information, engage with existing information-sharing communities, and make effective use of threat information to support the organization's overall cybersecurity practices.

4. Use the organizational form of PPPs that best fits one's needs:

The format of PPPs differs and they function in many different ways, varying from very informal types of cooperation to more formal partnerships. The degree of formality is often associated with the amount of control the governmental bodies aim to exert.

PPPs can provide some of the following benefits for CIP/CIIP:

- improved capacity of relevant CI/CII operators to response to cybersecurity incidents;
- more resilient CI/CII, leading to improved supply-chain resilience;
- improved capacity to maintain business continuity, resulting in higher levels of service and trust between service providers and clients;
- a higher level of understanding of how dependencies among sectors affect responses to
- emergencies, leading to better levels of preparation and response to disruptions, as well as shorter recovery periods; and
- reduced risks and lower costs for all organizations involved, owing to improved cooperation.

While there is no guaranteed format for success when establishing a PPP, it is vital to consider the following factors:

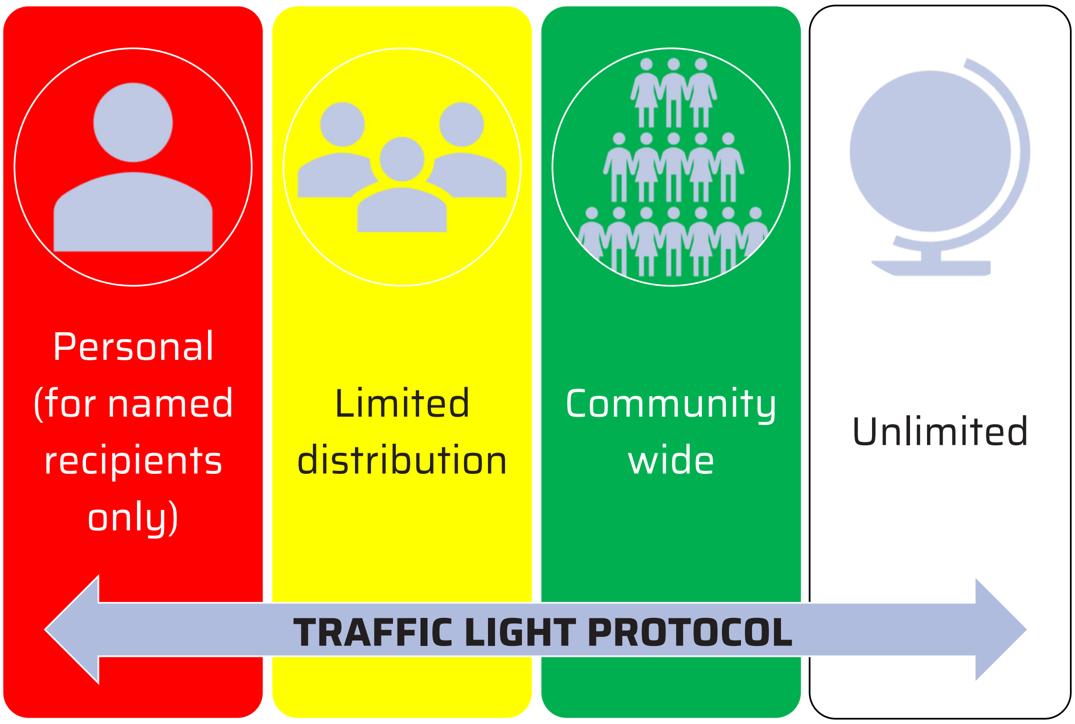
- **Trust:** As PPPs in CIP/CIIP often concern sensitive subjects (for example, in terms of commercial interests, reputation, security, or shifting responsibilities), it is essential to create an atmosphere of trust in which all organizations show awareness of each other's need for discretion and consistently act accordingly. Clear membership guidelines of operating rules may support the building of trust, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).
- **Value:** There must be clear benefits to participating in a PPP to ensure sustainable engagement rather than short-lived enthusiasm.
- **Respect:** All organizations have to recognize and respect the added value that the other organizations bring to the collaboration. This can be achieved by articulating your own added value, while actively looking for the added value of your partners.
- **Code of conduct:** It is necessary to have clear, specific, and predictable rules that do not provide scope for discretion and prevent any conflict of interest.

- **Awareness of each other's potential and restrictions:** This prevents misunderstandings and enables the alliance to be as effective as possible. This implies that both organizations should be familiar with the other's business and ideally have worked together for a long period of time, preferably years.
- **Realistic expectations:** All organizations should consider the affordability of resources, the development budget, and so on to be able to form realistic expectations of the PPP.

5. Ensure the discretion of shared information:

To establish the level of trust needed for information sharing between public and private organizations, it is necessary to establish procedures on how to deal with sensitive information in a way that maintains trust. The TLP provides a very easy method for establishing the required level of confidentiality for the information exchanged. One of the key principles of the TLP is that whoever contributes sensitive information also establishes whether and how widely the information can be circulated. The originator of the information can label it with one of four colours:

- **RED:** personal (for named recipients only). In the context of a meeting, for example, RED information is limited to those present at the meeting. In most circumstances, RED information is shared verbally or in person.
- **AMBER:** limited distribution. The recipient may share AMBER information with others within their organization, but only on a 'need-to-know' basis. The originator may be expected to specify any restrictions for accessing the information.
- **GREEN:** community wide. Information in this category can be circulated widely within a particular community; however, the information may not be published or posted publicly on the internet, nor released outside the community.
- **WHITE:** unlimited. Subject to standard copyright rules, WHITE information may be distributed freely, without restriction.



The TLP is used widely, by both nations and multinational working groups. Its strength is that it is very easy to use and the responsibilities of both the originator and receiver of the information are clearly defined.

IV. Examples of information-sharing initiatives

UP KRITIS (Germany)

In Germany, UP KRITIS is a national joint initiative between the state and CI operators for the protection of CII. UP KRITIS consists of more than 450 associates. As information and communication technology (ICT) has become an important element of all critical processes, the protection of information infrastructure is of particular importance to UP KRITIS. The organizations involved cooperate based on mutual trust, exchanging ideas and experiences and helping each other to learn how to effectively protect the critical (information) infrastructure.

MELANI (Switzerland)

MELANI serves two customer groups: an open customer group composed of private computer and internet users and small and medium-sized enterprises in Switzerland, and a closed customer group comprising selected operators of the national CI (such as energy suppliers, telecommunication companies, and banks). It is MELANI's responsibility to protect these CI, especially those that critically depend on the functioning of information and communication infrastructures – in other words, CII. The goal is to ensure that network and system interruptions, as well as abuses, are rare, of short duration, and controllable, and that they have minimal impact. MELANI can only achieve this task through close partnership and cooperation with these CII operators. In this partnership, MELANI focuses on sharing knowledge and resources that are available only to the government and "factor to success" not otherwise accessible to the private sector, especially information from intelligence services (for example, on countering industrial espionage), the National Computer Emergency Response Teams (CERTs), and law enforcement.

V. References and further reading

Klaver, M.H.A. 2021. GFCE CIIP Capacity Framework. Available at: https://cybilportal.org/wp-content/uploads/2021/08/GFCE-CIIP-Capacity-Framework.pdf.

GFCE (Global Forum on Cyber Expertise). 2022. Towards Identifying Critical National Infrastructures in the National Cybersecurity Strategy Process. Available at: https://cybilportal.org/wp-content/uploads/2022/03/White-Paper-Towards-Identifying-CNI-in-the-NCS-Process.pdf.

GFCE and the Meridian Process. 2016. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-makers. Available at: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

UK Foreign, Commonwealth & Development Office. 2021. 'Cyber-threat intelligence information sharing guide'. Available at: https://www.gov.uk/government/publications/cyber-threat-intelligence-information-sharing/cyber-threat-intelligence-information-sharing-guide.

NIST SP 800-150 Guide to Cyber Threat Information Sharing. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

✉ info@dcaf.ch
☎ +41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva