POLICY BRIEF

Strengthening National CSIRT Cooperation: from Domestic Setups to International Networks

DR SAMUELE DOMINIONI · HELENA HINKEL

Introduction

National computer security incident response teams (national CSIRTs or nCSIRTs)[1] play a significant role in international information communication technology (ICT) security and cooperation. This role has been repeatedly recognized by the United Nations Groups of Governmental Experts (GGEs) and Open-ended Working Groups (OEWGs) on international security and ICTs over the past decades.

In these contexts, States have underlined CSIRTs' unique responsibilities and functions in managing and resolving ICT incidents and their role in contributing to the maintenance of international peace and security. Given the relevance of CSIRTs for international security, one of the 11 voluntary norms of responsible State behaviour – norm 13(k) – specifically addresses CSIRTs and recognizes the importance of information-exchange and communication among national CSIRTs.

Such exchange and communication can be multilayered (i.e., spanning domestic, regional, and international levels), multifaceted (e.g., involving actors across a range of portfolios and sectors), and may involve a wide variety of processes, procedures, and key factors, such as trust, that may impact effective cooperation among different national CSIRTs. In fact, these teams may face several challenges when they engage in information-exchange and communication with other national CSIRTs. These challenges can often be traced back to how States have established, equipped, and maintained their national CSIRTs. Indeed, this policy brief argues that the capacity of national CSIRTs to engage internationally (bilaterally, regionally and globally) is highly dependent on their domestic implementation.

To support States in strengthening information-exchange and communication among national CSIRTs, this policy brief first examines the main characteristics of national CSIRTs and their relationships with other domestic CSIRTs. It then explores the domestic dimension of information-exchange and communication, including cooperation among national stakeholders, recurring challenges, and possible solutions. Finally, the brief outlines the main typologies of international cooperation for national CSIRTs, highlighting key challenges and illustrating selected good practices.

[1] The term CSIRT is the most commonly used general label for teams that handle cybersecurity incidents and comes without licensing restrictions. CERT (computer emergency response team), while historically significant and widely recognized, is a registered trademark of Carnegie Mellon University. Other naming conventions, such as NCSC (national cyber security centre), CDC (cyber defence centre), and CIRT (cyber incident response team), are also used in various contexts. Despite the variation in terms, these generally refer to teams performing comparable functions in the realm of cyber incident response and coordination. Here, the term CSIRT is used inclusively.

A note on the methodology

The research phase for the policy brief followed a two-stage approach. The first stage focused on literature review and desk research. It served to provide an overview of currently operating national CSIRTs, establish a first understanding of the different domestic setups globally, and offer insights into bilateral, regional, and international cooperation initiatives. The second stage of the research involved semi-structured interviews with a selection of national CSIRTs and international and regional networks. These were conducted to better understand the roles, mandates, and challenges of these entities, as well as the good practices they have developed when collaborating and cooperating at the domestic and international levels. Geographical representation was considered in selecting the participants.[2]

What is a National CSIRT

The establishment or designation of a national CSIRT as an authorized incident response authority is a State prerogative, and there is no universally agreed definition of what constitutes a national CSIRT, nor of its attributes and characteristics.

Notwithstanding the absence of such a definition, there is a shared understanding of what constitutes a national CSIRT. Typically, this is a team formally designated by national authorities, often a governmental entity, to serve as the central coordination point for ICT incident response at the national level. In the majority of cases, national CSIRTs operate as independent governmental organizations and with executive authority under the auspices of a wide range of existing governmental departments. As a result, the constituencies they serve can vary considerably. For example, some national CSIRTs have broad mandates and are responsible for coordinating incident response among all national stakeholders, including the government, network operators, the private sector, and the general public, while others serve only some, but not all, of these groups.[3] Nevertheless, their overarching role is to enhance a State's ICT safety, security, and protection. Consequently, their primary constituencies are national assets and users (such as critical infrastructure, domain names, citizens, etc.).

To strengthen national ICT posture, teams undertake various tasks, including managing and coordinating the national response to significant cybersecurity threats, providing early warnings, supporting capacity-building, and serving as an official point of contact for foreign CSIRTs and international networks.

[2] Interviews and open-ended surveys were conducted from June to August 2025 with participants from the national CSIRTs of Argentina, the Bahamas, Brazil, Brunei Darussalam, Canada, Italy, Japan, Mauritius, the Netherlands, Russian Federation, South Africa, and Sri Lanka, as well as with participants from the Cybersecurity Division/ITU, the African Forum of Computer Emergency Response Teams and the Forum of Incident Response and Security Teams.

[3] Interviews with Cybersecurity Division/ITU.

National CSIRTs are expected to maintain sufficient operational capabilities to be able to provide a set of both proactive and reactive functions, as well as preventive and educational services.[4] As such, these teams are an essential component of a national capacity to respond swiftly to and recover from cybersecurity incidents, minimizing adverse impacts and strengthening overall resilience.

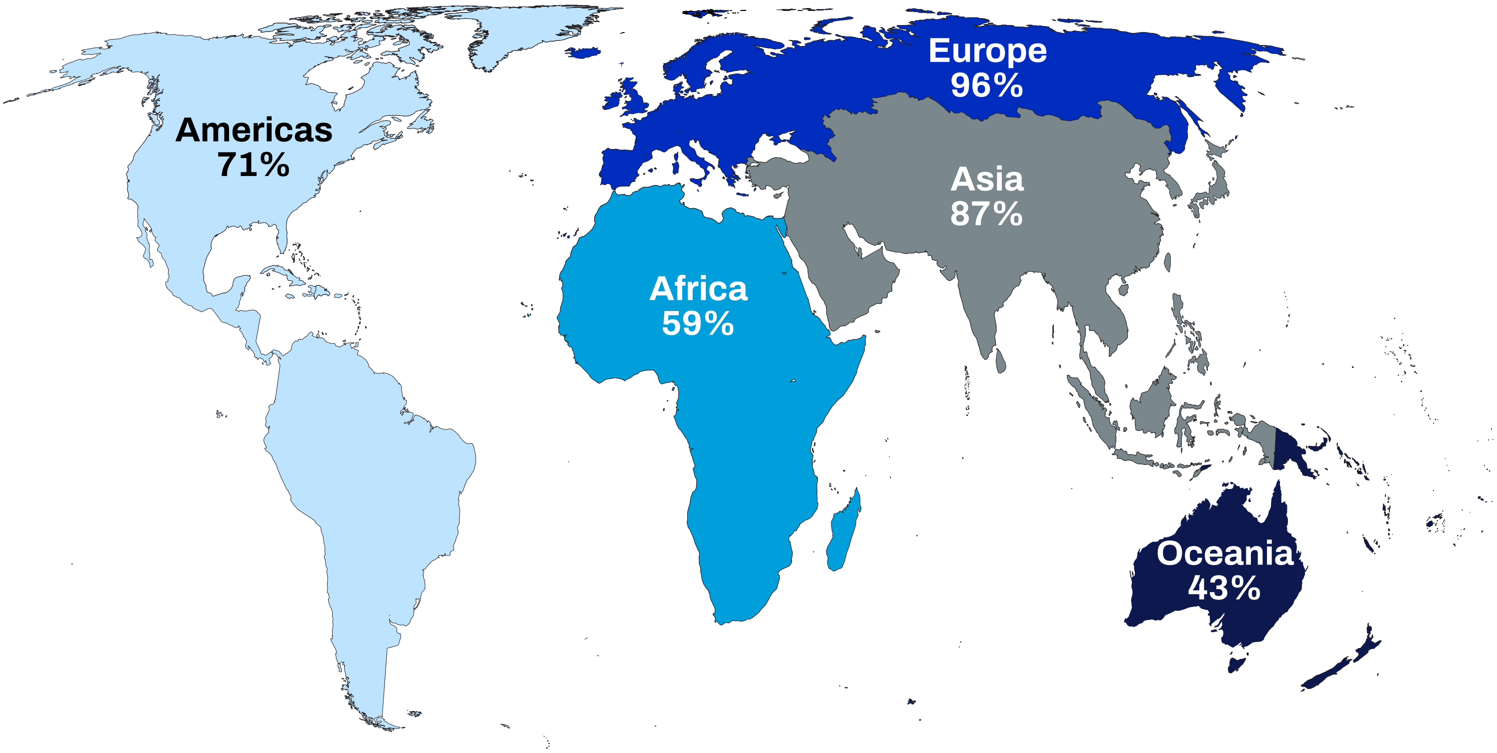
Regardless of their domestic implementation, which may differ in structure, mandate, or technical sophistication, national CSIRTs are often acknowledged internationally through their participation in regional or global networks such as the Forum of Incident Response and Security Teams (FIRST).

To summarize, some key characteristics of national CSIRTs include:

- being formally designated by a national authority, and operating under a government-approved mandate;
- providing a set of services to its constituencies (e.g., public institutions, network operators, general public);
- working to enhance the national ICT posture; and
- being acknowledged at the regional and international level.

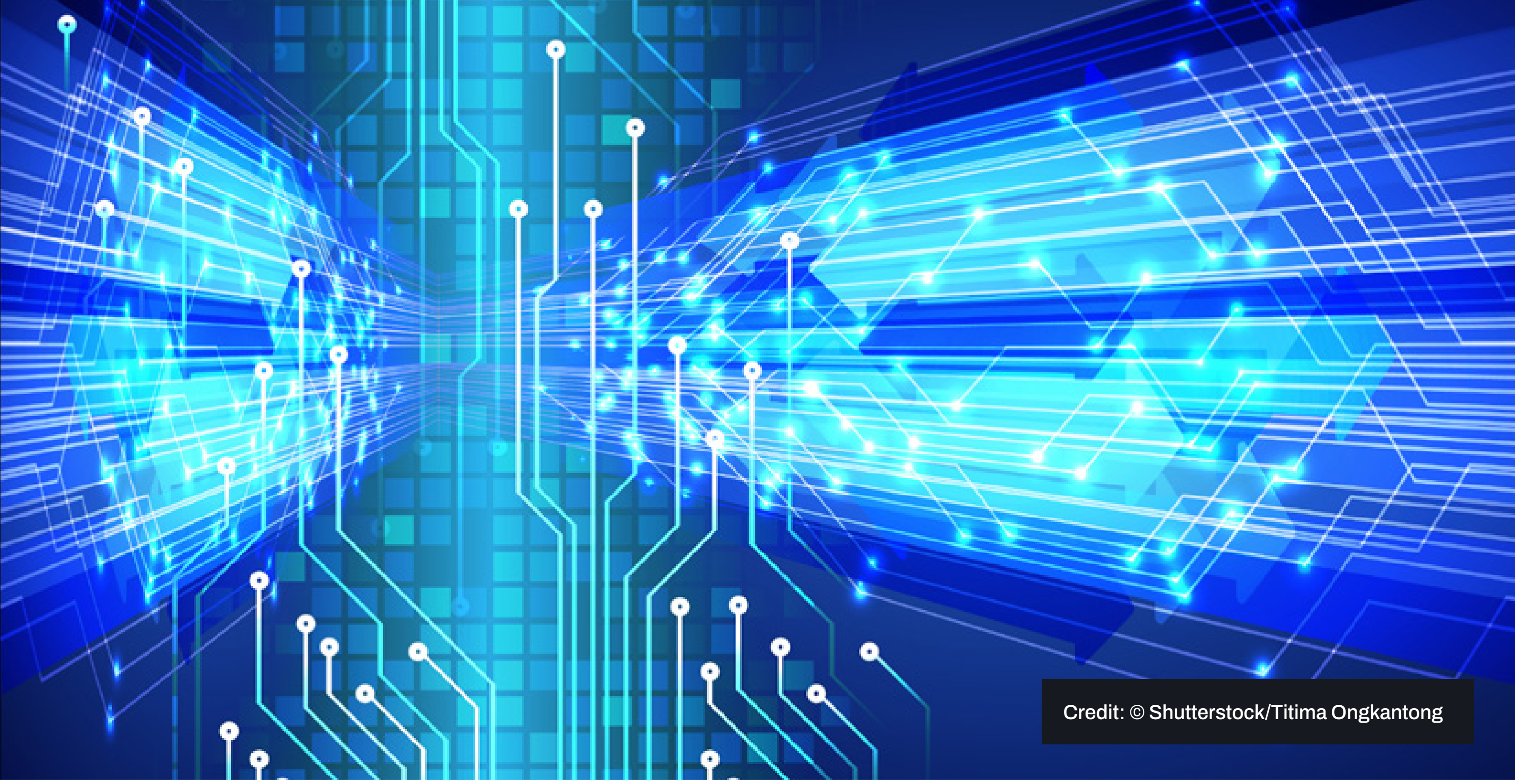
Despite their clear importance and the critical role they play for national security, not all States have established a national CSIRT (see annex).

FIGURE 1: PERCENTAGE OF NATIONAL CSIRT COVERAGE PER REGION



Geographic regions as per the United Nations M49 Methodology. The assignment of countries or areas to specific groupings is for statistical convenience and does not imply any assumption regarding political or other affiliation of countries or territories by the United Nations.

[4] ITU, World Bank et al. National Cybersecurity Strategy Guide. Forthcoming.



Credit: © Shutterstock/Titima Ongkantong

Other types of public CSIRTs

Besides national CSIRTs, there are other types of CSIRTs (see fig. 1) that may be present in the country (and beyond), each with a role and mandate to enhance ICT security. These include governmental, sectoral, and regional CSIRTs.[5] These other CSIRTs may be crucial actors with which national CSIRTs need to interact, particularly for coordinated incident response, threat intelligence sharing, and managing cross-border cyber incidents.

- **Governmental CSIRT**: are usually tasked with protecting the digital infrastructure of government entities, including ministries, public agencies, law enforcement, and critical services. They are typically embedded within or directly overseen by a governmental authority, such as a ministry of interior, defence, or telecommunications. Their responsibilities include monitoring threats to government networks, managing incidents affecting public institutions, and supporting policy implementation related to State cybersecurity. In many States, governmental CSIRTs operate alongside national CSIRTs, with clearly defined and complementary roles. In others, where there is no national CSIRT, governmental CSIRTs may fulfil the national coordination function, particularly in contexts where resources or expertise are limited.
- **Sectoral CSIRT**: are usually responsible for incident response and coordination within a specific sector, such as finance, health, energy, or telecommunications. In such a role, they may be considered CSIRTs with national-level responsibility.[6]

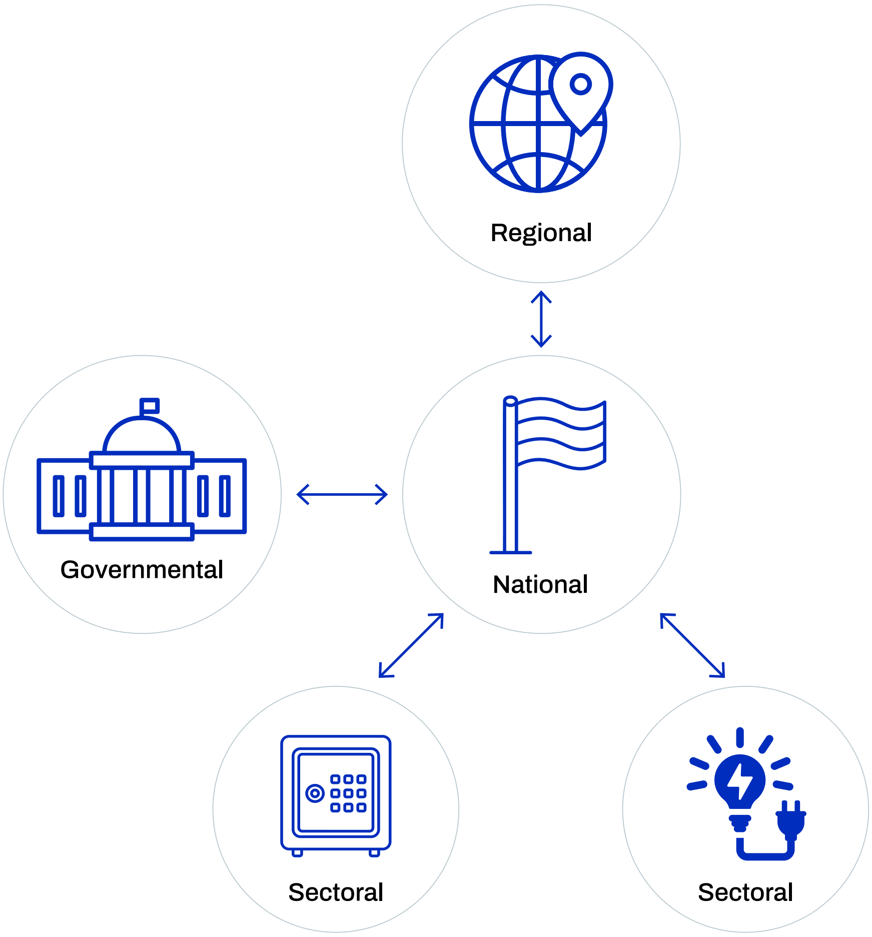
[5] This list is not exhaustive; for example, there are other public CSIRTs serving subnational polities, such as a province or city.

[6] This term was introduced by FIRST to describe domestic CSIRTs that, despite not being labelled national, are responsible for relevant industries or sectors considered critical for a country. In light of this, such CSIRTs can take part in FIRST's initiatives targeting national CSIRTs.

These teams are designed to address the cyber threats, regulatory requirements, and operational dispositions relevant to their sector. They can support incident detection, mitigation, and information-sharing, and often act as intermediaries between individual entities or companies and national or governmental CSIRTs.[7]

- **Regional CSIRT**: serve a group of States or jurisdictions within a certain geographical/political region. Typically, regional CSIRTs facilitate cross-border information sharing and provide technical assistance and training. In specific contexts, especially regions where cybersecurity capacity is uneven or still developing, they play a key role in supporting national and sectoral CSIRTs, including acting as a "CSIRT of last resort"[8] in specific cases.[9]

FIGURE 2: AN EXAMPLE OF AN ECOSYSTEM OF CSIRTS



[7] Interview with members of national CSIRTs.

[8] 'CSIRT of last resort' refers to the team that intervenes if no other competent or designated CSIRT is available to handle a cybersecurity incident.

[9] For example, the African Forum of Computer Emergency Response Teams can act as the last resort regarding security incidents relating to networks operated in the African Network Information Centre Service Region.

Credit: © Shutterstock/Imilian

Domestic CSIRT cooperation

Cooperation with other domestic CSIRTs is an essential asset for national CSIRTs.[10] Through such cooperation, national CSIRTs can enhance their awareness and readiness to specific threat landscapes, as well as their capacity to coordinate in the event of an ICT incident. Collaboration and trust between stakeholders and the national CSIRT are developed through time and leveraged in times of crisis. Cooperation may involve multiple public CSIRTs (e.g., a sectoral CSIRT and the national CSIRT) or other private or non-governmental CSIRTs (e.g., CSIRTs operating within academic institutions, telecommunications companies, ICT service providers and vendors, or within other major private sector organizations).

Domestic cooperation with other CSIRTs can be categorized as formal or informal:

- **Formal cooperation** usually involves an official commitment to cooperate, established by requirements set in a formalized agreement or other mechanism of cooperation. Moreover, formal cooperation may include reporting obligations to the national CSIRT that other domestic CSIRTs must adhere to, and that are required by law.
- **Informal cooperation** occurs without official agreement or legal requirement; it relies, instead, on personal relationships, professional networks, and mutual understanding of roles and responsibilities across the teams' domestic landscapes.

[10] For a few States, the national CSIRT is the only CSIRT in the country. This section is relevant only where there is more than one CSIRT at the national level.

Formal and informal cooperation dynamics often coexist. Informal engagement, especially built through personal relationships, is usually the first channel of communication between domestic CSIRTs.

Both formal and informal domestic cooperation may pose challenges that, in turn, impair the capacity of national CSIRTs to perform their functions effectively. They include the following.

1. **Lack of trust**:
   This is a widespread and systemic issue that affects national CSIRTs across the world, regardless of the type of cooperation in place. Without trust among the CSIRTs, information-sharing and other cooperative activities are impaired. Lack of trust might be caused by several factors, including concerns about reputational damage in sharing information about incidents, competition over scarce resources (e.g., funding), or excessive securitization of the national CSIRT (e.g., affiliation to or integration with the defence sector).
2. **Weak institutional setup**:
   This challenge is particularly relevant in CSIRT landscapes where there are no formal cooperation mechanisms in place. The national CSIRT must therefore rely on the voluntary sharing of information from other domestic CSIRTs. Lack of trust, lack of shared understanding of the roles and responsibilities of actors (e.g., the role of the national CSIRT in case of an incident), and fragmented information on the CSIRT landscape (e.g., numbers of active CSIRTs in the country or how to contact the national CSIRT) can weaken the information-sharing process with the national CSIRT.
3. **Differing Stages of Development and Organizational Models**:
   Domestic CSIRTs may have differing degrees of operational maturity, as well as organizational models—for example, unequal incident-handling capacity (such as technical expertise and staffing), dissimilar or unduly restrictive confidentiality standards, or a lack of common templates for information-sharing. These diversities can significantly reduce the effectiveness of cooperation, which is vital in cases of major cyber incidents, when a swift and harmonized national response is needed.

States, through their national CSIRTs, may tackle some of these challenges by adopting good practices, including the following.

1. **Building a CSIRTs community**:
   This is a crucial aspect to foster trust, coordination, and shared understanding of the CSIRT landscape, including the roles and responsibilities of all participants. Such an initiative could include mapping the domestic CSIRTs and establishing regular interactions through national forums or joint exercises, which help develop personal relationships and confidence. Ideally, to foster a greater sense of belonging among domestic CSIRTs, such initiatives should be taken with a bottom-up rather than a top-down approach.[11]

[11] Interview with a national CSIRT member.

2. **Strengthening institutional foundations**: This can be achieved by equipping national CSIRTs with the appropriate mandate and authority to perform their role and functions. In this regard, it is good practice to provide the national CSIRT with a legal framework that strengthens its authority in requesting information, dealing with incidents, and setting standards and procedures for domestic cooperation. Additionally, the flow of information can be facilitated by raising awareness on the importance of information-sharing for quick and harmonized responses to cyber incidents, creating a list of points of contact for all domestic CSIRTs, and providing swift responses or feedback to queries.

3. **Harmonizing the CSIRTs' Landscape**: Diversity in terms of organization and processes across domestic CSIRTs results from the diversity of their roles and responsibilities. Nevertheless, using similar taxonomies to categorize incidents, compatible confidentiality standards, and standardized procedures and templates can improve coordination and common responses in cases of cyber incidents.

Table 1. Summary of Key Challenges and Good Practices

CHALLENGES	GOOD PRACTICES
1. Lack of trust	1. Building a CSIRTs community
2. Weak institutional setup	2. Strengthening institutional foundations
3. Differing Stages of Development and Organizational Models	3. Harmonizing the CSIRTs' Landscape

Credit: © Shutterstock/piggu

Credit: © Shutterstock/Tommy Ajrul Naim

International CSIRT Cooperation

Given the cross-border nature of cyber threats, cooperation among national CSIRTs is crucial to an effective response. Through international cooperation, national CSIRTs can share a wide variety of relevant information, including technical data (e.g., indicators of compromise); coordinate joint responses to cyber incidents; develop common good practices to manage and enhance cybersecurity; as well as assist other national CSIRTs in need (e.g., through capacity-building activities).

International cooperation can be established through bilateral, regional, and global partnerships.

Bilateral cooperation: refers to direct interactions between two national CSIRTs, usually established through a memorandum of understanding. Generally, bilateral cooperation is agreed between States that already have established relations and trust. Bilateral cooperation is often operational (for example, focusing on rapid and confidential information-exchange).

- **Regional cooperation**: rrefers to interactions among national CSIRTs within a geographical or political region, or between a national and a regional CSIRT. There are several examples of regional cooperation with varying levels of institutionalization (e.g., APCERT, CSIRT America Network, and EU CSIRT Network). Usually, regional cooperation aims at strengthening information-sharing, capacity-building, and mutual support among neighbouring States.
- **Global cooperation**: refers to interactions among national CSIRTs through global networks of CSIRTs[12] or with international

[12] There is no single, dedicated global network exclusively for national CSIRTs. There are mixed networks of CSIRTs (including private and other types), such as FIRST and Trusted Introducer, that bring together national CSIRTs from many countries worldwide.

organizations such as the International Telecommunication Union.[13] Such cooperation is more focused on facilitating information-exchange, capacity-building, and building trust and recognition through accreditation or certification standards.

When national CSIRTs engage in international cooperation, they may encounter the following challenges, particularly when working with counterparts with whom they have less-established relationships.

1. **Lack of trust**: this is a systemic challenge, just as at the domestic level, but even more acute for international cooperation. Several factors can contribute to a low level of confidence among States, including politicization of technical cooperation (e.g., a State may refrain from cooperating with others whose foreign policy objectives diverge from its own), excessive securitization (e.g., not cooperating with other national CSIRTs because of national security imperatives), or high-turnover in national CSIRT staff (e.g., employees with established relationships with other national CSIRTs leave or change roles).
2. **Self-interest over collaboration**: it refers to instances when national CSIRTs are guided exclusively by uncooperative principles, such as sovereign interests. This may give rise to transactional approaches to information-sharing (e.g., a national CSIRT shares information shaped by a quid pro quo dynamic) or to selective/situational cooperation (e.g., a national CSIRT may decide to respond to a request for assistance from another CSIRT only when an incident is spreading to its own constituency).
3. **Procedural challenges**: this refers to a wide variety of issues related to both interactions among national CSIRTs and the aspects of domestic implementation involved in the international cooperation efforts. Concerning the former, challenges may include language barriers, contrasting data privacy regulations, and different methods for incident classification. The latter set of challenges may refer to slow domestic coordination or procedures for responding to requests for assistance/information-sharing (e.g., long procedures set by other mutual agreements), absence of inter-agency relations (e.g., no interaction between national CSIRT and the Ministry of Foreign Affairs), weak institutional implementation at the domestic level (see section above), and differing levels of expertise and capacity (e.g., one party's tools may be outdated).

States and National CSIRTs engaging in international cooperation may consider the following good practices to tackle some of the identified challenges.

1. **Build an international network**: to enhance trust among peers in other countries. For example, it is crucial that national CSIRTs connect and engage with regional and international partners and networks, as building trust and confidence takes time and

[13] Within the United Nations system, the International Telecommunication Union (ITU) is the specialized agency mandated to support Member States in strengthening their information and communication technology infrastructures and cybersecurity capacities. In line with this mandate, ITU works with Member States to build capacity at national and regional levels, deploy cybersecurity capabilities, conduct cyber drills to enhance readiness and coordination, and assist in establishing and enhancing national CIRTs. The ITU CIRT framework guides engagement with beneficiary States in assessing, developing, and deploying the technical capabilities and training required to establish national CIRTs.

may necessitate sharing experiences and, as well, some cultural adjustment. These engagements, including in-person meetings, certifications, and joint exercises, can help to foster relationships and confidence among national CSIRTs. Moreover, as outlined in the GGE 2021 report, it is essential for governments to avoid the politicization of CSIRTs and to respect the independent character of their functions.[14] Considering this, States should outline clear status, authority, and mandates of national CSIRTs (distinguishing their unique and neutral functions from other government functions) in their cybersecurity policy and/or strategy. Finally, initiatives to strengthen national CSIRTs cooperation can be considered by the international community, including through the Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs.

2. **Establish ethical standards**: states should consider establishing ethical and regulatory frameworks specific to the work of national CSIRTs, setting fundamental principles and standards for their operations. These should be developed in line with international guidelines and standards (e.g., the FIRST Code of Ethics).

3. **Strengthen domestic setup**: international cooperation is often hindered by domestic procedural inefficiencies. There is a wide range of good practices to address some of the procedural challenges listed above. For example, consider establishing a (multilingual) focal point within the national CSIRT to deal with international requests. Moreover, it should be taken into account to establish a channel of communication between the national CSIRT and the Ministry of Foreign Affairs to reinforce international coordination. In addition, national CSIRTs should consider adopting existing common approaches, such as for incident classification or communication templates (or develop new common approaches with peers). Addressing domestic flaws and weaknesses helps to ensure smooth engagement with international partners.

Table 2. Summary of Key Challenges and Good Practices

CHALLENGES	GOOD PRACTICES
1. Lack of trust	1. Build an international network
2. Self-interest over collaboration	2. Establish ethical standards
3. Procedural challenges	3. Strengthen domestic setup

[14] These include the domains of operation and ethical principles that guide the work of authorized emergency response teams.

Credit: © Shutterstock/nednapa

Conclusions

National CSIRTs are recognized as critical players in international cybersecurity. Their role has evolved over time, and they are now well-established actors in many States' cybersecurity systems, handling multiple tasks and responsibilities.

Nevertheless, not all national CSIRTs have the same capacity to engage with activities both domestically and internationally. One of the major issues that inhibits effective cooperation at both levels is trust. This is a systemic challenge because, without trust, information does not flow. As such, a lack of trust can fragment domestic and international communities, especially in the event of a cyber incident, considering that "in crisis, information flows through trusted networks first".

Building an environment of mutual trust where national CSIRTs can effectively share information starts at the national level. Consequently, this policy brief identifies a range of characteristics and good practices that could help States to establish and equip an effective national CSIRT, including building confidence both at the domestic and international levels of operation. Moreover, this policy brief can guide governments in implementing norm K of the Framework of Responsible State Behaviour in cyberspace, ultimately contributing to a more secure and stable ICT environment.

Annex.
States with a National CSIRT as of August 2025[15]

Afghanistan

Albania

Algeria

Andorra

Argentina

Armenia

Australia

Austria

Azerbaijan

Bahamas (The)

Bahrain

Bangladesh

Barbados

Belarus

Belgium

Benin

Bhutan

Bolivia
(Plurinational State of)

Botswana

Brazil

Brunei Darussalam

Bulgaria

Burkina Faso

Cambodia

Cameroon

Canada

Chile

China

Colombia

Costa Rica

Côte d'Ivoire

Croatia

Cuba

Cyprus

Czechia

Denmark

Djibouti

Dominican Republic

Ecuador

Egypt

Estonia

Eswatini

Ethiopia

Finland

France

Gambia (Republic of The)

Georgia

Germany

Ghana

Greece

Grenada

Guatemala

Guyana

Hungary

Iceland

India

Indonesia

Iran (Islamic Republic of)

Iraq

Ireland

Israel

Italy

Jamaica

Japan

Jordan

Kazakhstan

Kenya

Kuwait

Kyrgyzstan

Lao People's Democratic
Republic

[15] The list was compiled from open-source databases, including ITU, FIRST, Trusted Introducers, as well as official regional networks. There are cases where a governmental CSIRT is considered to cover also national CSIRT functions; as such these cases are included in the list. A few States (e.g., Fiji) are currently in the process of setting up their national CSIRT; they were not included in this list.

Latvia

Libya

Liechtenstein

Lithuania

Luxembourg

Malawi

Malaysia

Malta

Mauritius

Mexico

Monaco

Mongolia

Montenegro

Morocco

Mozambique

Myanmar

Namibia

Nepal

Netherlands
(Kingdom of the)

New Zealand

Nigeria

North Macedonia

Norway

Oman

Pakistan

Panama

Papa New Guinea

Paraguay

Peru

Philippines

Poland

Portugal

Qatar

Republic of Korea

Republic of Moldova (The)

Romania

Russian Federation

Rwanda

Samoa

Saudi Arabia

Serbia

Seychelles

Sierra Leone

Singapore

Slovakia

Slovenia

Somalia

South Africa

South Sudan

Spain

Sri Lanka

Sudan

Suriname

Sweden

Switzerland

Syrian Arab Republic

Thailand

Timor-Leste

Togo

Tonga

Trinidad and Tobago

Tunisia

Türkiye

Uganda

Ukraine

United Arab Emirates

United Kingdom of Great
Britain and Northern Ireland

United Republic of Tanzania

United States of America

Uruguay

Uzbekistan

Vanuatu

Venezuela,
Bolivarian Republic of

Viet Nam

Zambia

Acknowledgements

Support from UNIDIR funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Security and Technology Programme (SECTEC), which is supported by Czechia, Germany, Italy, the Netherlands, Norway, Switzerland, and Microsoft. SECTEC's Cyber Workstream is also supported by France.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Authors

Dr. Samuele Dominioni is a senior researcher in the Security and Technology Programme at UNIDIR.

Helena Hinkel was a former graduate professional in the Security and Technology Programme at UNIDIR.

Citation

S. Dominioni and H. Hinkel. *Strengthening National CSIRT Cooperation: from Domestic Setups to International Networks*. Geneva, Switzerland: UNIDIR, 2025.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual author. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

Cover photography: AdobeStock/DC Studio. Design and layout by Kathleen Morf.

UNIDIR

𝕏 @unidir

in /unidir

/un_disarmresearch

f /unidirgeneva

▶ /unidir

Palais de Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG