POLICY BRIEF

Signals in the Noise

Building Governmental Capabilities to Detect Cybersecurity Threats

Christina Rupp

November 27, 2025

Tech analysis and policy ideas for Europe

interface

Table of Contents

Executive Summary

Amid an evolving cyber threat landscape, governments are facing increasing pressure to strengthen their capabilities to detect cybersecurity events and incidents. Detection—the ability to spot signals of malicious activity throughout the noise of billions of daily digital interactions—is a cornerstone of effective cybersecurity. While some countries and regions, including the EU, have taken steps to prioritize detection capability development, many still lack the necessary policies, legal frameworks, tools, and skills to monitor and analyze threats within their jurisdictions.

In general, states have become more outspoken about the shortcomings and gaps in their detection capabilities. Yet, detection has not been prominently reflected in multilateral international cybersecurity policy discussions so far, particularly cyber diplomacy debates at the United Nations. While some international assistance exists to help states build these capabilities, such efforts remain fragmented and have yet to receive the policy attention they deserve.

This is a missed opportunity for several reasons. Bolstering detection capabilities internationally represents untapped potential for the EU, its Member States, and other countries with advanced cybersecurity capabilities. It would be in their interest to recognize detection as a matter of strategic importance, assist states with less mature capabilities in this area, and elevate the issue on the cyber diplomacy agenda. Such an approach would generate multiple, mutually reinforcing benefits:

- **It boosts the resilience of partner countries.** Advancing detection capabilities in partner countries elevates their cyber resilience by improving the identification of existing and emerging threats, pinpointing preventive gaps, and refining forensic analysis for more effective incident response.
- **It enhances collective security.** As detection capabilities grow, a state's national situational awareness also improves. By heightening this awareness, states become better able to identify malicious cyber activities and ultimately also attribute them to specific threat actors. This, in turn, can promote accountability and strengthen collective security among countries facing shared threats.
- **It supports the implementation of UN cyber norms.** Because detection capabilities are a key enabler for implementing many of the international community's agreed norms of responsible state behavior in cyberspace, helping partner countries build these capabilities improves their ability to comply with these political commitments. In doing so, donor countries can also foster greater convergence on how these collective behavioral expectations can be operationalized in practice.

This paper serves as a practical resource for policymakers seeking to act on this strategic opportunity by linking operational realities, technological developments, policy considerations, and diplomatic efforts. It distinguishes between two core

components of governmental detection capability and analyzes the factors that enable states to fulfill these responsibilities: (1) **monitoring and analyzing the operational environments of individual public sector entities**, and (2) **fostering detection across a country's broader digital ecosystem**, including both governmental and private infrastructure, **and across national jurisdictions**. Policymakers in donor countries, together with their counterparts in partner countries, can use these insights to identify gaps, set priorities, and design targeted support measures.

The paper concludes with three overarching considerations rather than specific recommendations, as appropriate international detection capability-building actions will always be determined by each partner country's needs, context, and existing capabilities:

- **Basics first**: Activities should be aimed at developing detection capabilities gradually, starting with foundational policy, governance, and organizational measures before progressing to more advanced measures.
- **Leverage unique added value**: Capability development should focus on areas where public-sector action can have the highest long-term impact to fulfill governmental detection responsibilities and leverage existing external resources for specific, noncritical tasks.
- **Invest in human expertise and community building**: Governments should prioritize fostering a diverse cybersecurity talent pipeline and trusted networks to ensure that detection capabilities are sustained and their impact is amplified beyond the duration of specific assistance programs.

By recognizing and acting upon the strategic value of detection capability-building, the EU and its Member States can advance their objective of aligning cyber capacity-building with UN cyber norms while generating the additional benefit of raising external awareness of the relevant EU acquis and deepening collaboration with like-minded partners.

Introduction

Amid an evolving cyber threat landscape and rising risks driven by the advancing sophistication of threat actors, among other factors, governments are facing increasing pressure to strengthen their abilities to detect cybersecurity events[1] and incidents.[2] Therefore, high-level policymakers are also increasingly recognizing the

1 A cybersecurity event is defined as "an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security," Australian Cyber Security Centre (2025): Guidelines for cybersecurity incidents. A detected security event might not turn out to be an actual incident after analysis, for example, legitimate user activity that resembles malicious activity.

2 Different to a cybersecurity event, a cybersecurity incident is defined as "an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations," Australian Cyber Security Centre (2025): Guidelines for cybersecurity incidents .

need to observe and analyze signals of malicious activity throughout the noise of billions of daily digital interactions. The need is further reflected in strategic planning and legislation, focusing, for example, on accelerating incident detection within government infrastructures, mandating detection-related measures for specific entities, or strengthening the ability to identify and thereby deter threat actors.

Four examples of the last few years:

- **United States**: In May 2021, then U.S. President Biden signed **Executive Order 14028 on Improving the Nation's Cybersecurity**.[3] The order underscores that "the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security" and outlines steps for the U.S. federal government to accelerate its capabilities.[4] In the area of detection, the order stipulates that "the Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks" and, inter alia, mandates the establishment of a so-called "Endpoint Detection and Response (EDR)[5] initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure."[6] Thus far, this policy has largely been sustained by the Trump administration.
- **United Kingdom**: Relevant UK strategies underscore that detection capabilities are vital for the UK's external and internal security. The UK's most recent **National Cyber Strategy** (2022) identifies "detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace" as one of its five pillars.[7] Looking inward, the UK's **Government Cyber Security Strategy** (also published in 2022) highlights "detecting cyber security events" as one of its seven priorities.[8] Among its objectives for 2025–2030 is the scaling of detection capabilities across government organizations, including the goal that "every government digital system [...] have 24/7 security monitoring."[9]
- **European Union**: Detection is also being progressively included in recent EU legislation in two ways. On the one hand, the EU has taken measures to increase detection capabilities within and across EU Member States. For example, the **EU's Cyber Solidarity Act** (CSOA),[10] which entered into force in February 2025 establishes a European Cybersecurity Alert System. This network of national and several cross-border "cyber hubs" of three or more national hubs aims to "build and enhance

3 In addition, as one of the last measures of his administration, Biden signed Executive Order 14144 on Strengthening and Promoting Innovation in the Nation's Cybersecurity in January 2025, which directs the "Secretary of Homeland Security, acting through the Director of CISA, [... to] develop the technical capability to gain timely access to required data from FCEB agency endpoint detection and response (EDR) solutions and from FCEB agency security operation centers" to facilitate "timely hunting and identification of novel cyber threats and vulnerabilities across the Federal civilian enterprise," among other objectives, Executive Office of the President (2025): Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity. Despite other changes to Executive Order 14144, its detection-related policies have also largely been sustained by the Trump Administration thus far.

4 Executive Office of the President (2021): Executive Order 14028: Improving the Nation's Cybersecurity.

5 "The term "endpoint detection and response" means cybersecurity tools and capabilities that combine real-time continuous monitoring and collection of endpoint data (for example, networked computing device such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities," Executive Office of the President (2025): Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity.

6 Executive Office of the President (2021): Executive Order 14028: Improving the Nation's Cybersecurity.

7 UK Government (2022): National Cyber Strategy 2022.

8 UK Government (2022): Government Cyber Security Strategy: 2022 to 2030.

9 UK Government (2022): Government Cyber Security Strategy: 2022 to 2030.

10 Regulation laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents (Cyber Solidarity Act), 2025/38.

coordinated detection and common situational awareness capabilities" (Art. 1(1), point (a)). Participation is voluntary for EU Member States (Art. 3(1)) and they can receive financial support from EU funds[11] to ensure that they have the necessary capabilities in place to participate if interested (Art. 9). On the other hand, the EU is increasingly placing obligations on specific entities to implement detection-related measures to strengthen their cybersecurity posture. For instance, the **Digital Operational Resilience Act** (DORA)[12] requires financial entities to take steps towards detecting potentially adverse activities and regularly testing measures taken (see further, e.g. Art. 10).[13]

- **Germany**: In June 2025, during his visit to Israel, German Minister of the Interior Alexander Dobrindt called for the establishment of a so-called **"Cyber Dome"** for Germany and expressed interest in learning from Israel in this regard.[14] Drawing an analogy to its Iron Dome, Israel's National Cyber Directorate has been operating a Cyber Dome since 2011, which monitors and analyzes the Israeli internet in real time.[15] The proposal for a German Cyber Dome was reiterated as one of three policy areas for enhancing cybersecurity, as adopted by the new German Federal Government in August 2025.[16] However, despite these announcements, as of November 2025, it remains unclear which specific measures and activities the German government plans to include in its proposed Cyber Dome initiative.[17]

These policy developments illustrate that detection capabilities are foundational to effective cybersecurity. They not only facilitate the discovery of anomalous activity, but also reflect a continuous process within a governmental cybersecurity strategy, serving a wide array of objectives and functions:

- Enabling network visibility and providing an understanding of both the current and historical state of systems and network activity, supporting national situational awareness and the identification of ongoing and emerging threats;
- Facilitating the evaluation and continuous improvement of preventive measures by highlighting what existing defenses may have missed, which can inform policies and investment planning by clarifying the specific threats public sector entities need to protect against (*connection to prevention*); and

11 See, for example, European Cybersecurity Industrial, Technology and Research Competence Centre (2025): Call for Expressions of Interest and European Commission (2023): Annex to the Commission Implementing Decision amending the Commission Implementing Decision C (2023) 1862 final on the financing of the Digital Europe Programme and the adoption of the work programme for 2023 - 2024.

12 Regulation on digital operational resilience for the financial sector (Digital Operational Resilience Act), 2022/2554.

13 Another example of highly relevant EU action is the NIS 2 Directive which lists "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" (Art. 11(3), point (a)) as the first of multiple tasks to be carried out by national Computer Incident Response Teams (CSIRTs), which each Member State must establish in order to comply with the Directive, Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 2022/2555.

14 DIE ZEIT, dpa, AFP, and Sven Crefeld (29.06.2025): Dobrindt fordert einen Cyber Dome für Deutschland, DIE ZEIT. See also Sven Herpig (25.09.2025): Ein Cyber Dome made in Germany?, Tagesspiegel Background.

15 Benjamin Stiebel (01.07.2025): Nach Dobrindt-Besuch in Israel: Kommt der Cyber Dome auch nach Deutschland?, Tagesspiegel and Israel National Cyber Directorate (2022): Gaby Portnoy, Director General of Israel National Cyber Directorate at CyberWeek: We are Promoting a National Cyber-Dome.

16 Bundesministerium des Innern (2025): Stärkung der Cybersicherheit – Kabinett beschließt Eckpunkte zur Erhöhung der Cybersicherheit.

17 In response to a parliamentary inquiry in the Bundestag concerning the financial and human resources allocated to the Cyber Dome, as well as the anticipated timeline for its implementation and operation, the Federal Ministry of the Interior solely indicated in July 2025 that it regards the Cyber Dome as a holistic program composed of numerous individual projects. According to the Ministry, several subprojects—such as a portal operated by the BSI, a reporting and information platform, and a system for the automated exchange of Indicators of Compromise (IoCs)—have already been initiated and received funding. Additional financial and human resources, however, would be subject to the ongoing budgetary process, Deutscher Bundestag (2025): Schriftliche Fragen mit den in der Woche vom 21. Juli 2025 eingegangenen Antworten der Bundesregierung, Drucksache 21/982.

- Serving as a trigger for initiating incident response and providing a source of evidence that supports forensic investigations and analysis of incidents (*connection to response*).

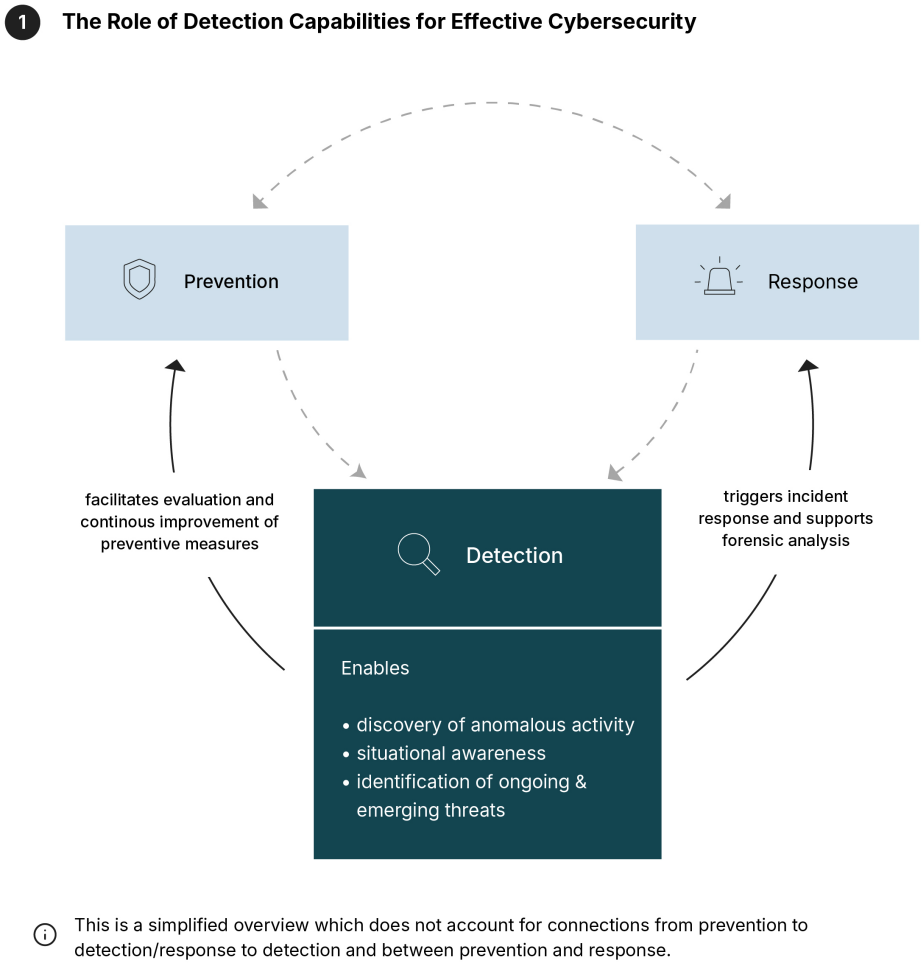


Figure 1: The Role of Detection Capabilities for Effective Cybersecurity

The policy developments also indicate that governments face various responsibilities and many feel the need to further develop strategies and strengthen legislative frameworks to better detect anomalous behavior. They also highlight a clear need for action and compliance from a wide range of actors, from public sector institutions to individual entities operating within a country's jurisdiction, to implement these commitments effectively. As a result, governments face numerous "to-dos" in accelerating their capacity to detect anomalous behavior, whether by following through on existing commitments made or by establishing the necessary policies and legal frameworks in the first place.

In addition to taking steps towards building their own detection capabilities, some states and other players are also engaging in international assistance measures in selected partner countries that also have a detection component. For example, such

efforts can include those aimed at building relevant institutional structures like national Computer Security Incident Response Teams (CSIRTs)[18] or Security Operations Centres (SOCs).[19] For many years, states have also progressively collaborated with each other through CSIRT-to-CSIRT cooperation formats, exchanging detection-relevant data and contextual information at the technical level, including in military settings.

Nonetheless, the integration of detection into UN-level cyber diplomacy debates has remained limited. Although cybersecurity has been on the UN agenda for a quarter-century, the capacity to detect cybersecurity incidents was mentioned in a relevant report for the first time only in 2021. The reports from relevant UN fora discussing cybersecurity—most recently the UN Open-ended Working Group (UN OEWG) on security of and in the use of information and communications technologies—mention them only in passing together with other capabilities.

While states agreed by consensus in these reports, inter alia, on the increased vulnerability arising from inadequate detection capacities[20] and recommended it as one priority area for international capacity-building,[21] there is no elaboration on what these capabilities entail or how they could contribute to advancing responsible state behavior. The modest attention to date likely reflects a combination of various factors, including the perception of detection as a primarily technical and operational concern rather than an international security issue. The marginal uptake since 2021 may also be a result of the growing number of states participating in UN cybersecurity discussions, which expands the pool of countries that may face gaps in this area.

This policy paper argues that the limited strategic and dedicated focus given to the development of detection capabilities and related international capability-building in cyber diplomacy circles represents an overlooked opportunity. Detection capabilities provide a prime example of where operational realities, technological developments, policy considerations, and diplomatic efforts can intersect and inform

18 FIRST defines a CSIRT as "an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission," FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

19 The UK NCSC defines a SOC as "a centralised facility within an organisation, responsible for activities such as security monitoring and incident management," UK National Cyber Security Centre (n.d.): Glossary.

20 The OEWG I final report underscored that "a lack of awareness and adequate capacities to detect, defend against or respond to malicious ICT activities may make them more vulnerable," (United Nations (2021): Open-ended working group on developments in the field of information and telecommunications in the context of international security (A/AC.290/2021/CRP.2)), which has been reiterated in the second (2023) and third (2024) annual progress reports (APRs) of the OEWG II as well as its final report (2025): United Nations (2023): Developments in the field of information and telecommunications in the context of international security (A/78/265); United Nations (2024): Developments in the field of information and telecommunications in the context of international security (A/79/214); and United Nations (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257).

21 The GGE 2021 report included "building or enhancing the technical, legal and policy capacities of States to detect, investigate and resolve ICT incidents" as one its recommended areas for international capacity-building, United Nations (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

each other to generate synergies. For this reason, this paper offers a practical resource for cyber diplomats and policymakers working on international cybersecurity policy who are interested in tapping into this potential. It is aimed at supporting them in translating highly technical needs and requirements for building detection capabilities into actionable strategies for strengthening these capabilities at the international level and enhancing collective resilience.

To do so, the paper first makes the case for why cyber diplomats should care about supporting partner countries in developing incident detection capabilities (Chapter 3). It then addresses how states can do so by defining capability-building[22] and discussing the two core responsibilities that make up a governmental detection capability (Chapter 4). Subsequent chapters explain what these responsibilities involve by walking through (some of) the procedural mechanisms, technical tools, and human expertise that public-sector entities need to take on these responsibilities (Chapters 5 and 6) and illustrating how some international initiatives are already implementing detection capability-building in practice (Chapter 7). The analysis then highlights key challenges governments face in developing and enhancing these capabilities (Chapter 8) before concluding with overarching considerations for policymakers in donor countries for designing activities aimed at strengthening detection capabilities across the globe (Chapter 9).

Why Cyber Diplomats Should Care About Building Detection Capabilities Across the Globe

Governments across the board—from small island developing states to members of the Group of Seven (G7)[23] —have expressed interest in detection, are actively seeking to enhance their capabilities, or have already taken political steps at the highest levels. Thus, developing and enhancing detection capabilities offers great potential for international assistance measures.

For interested donor governments, building detection capabilities in other states offers to address various differentiated objectives at once:

First, detection capability-building **furthers an essential cybersecurity capability in a partner country,** addressing a need progressively expressed by many countries. For

22 For a distinction between the terms capacities and capabilities, see Chapter 4.
23 See also Jacob Rudolph, Angus MacKellar and the G7 Research Group (2025): 2024 G7 Apulia Summit Interim Compliance Report.

all countries, having these capabilities is fundamental from a technical perspective, as they also provide insight into what to defend against and support the fine-tuning of their responses to emerging risks. For instance, South Africa called "posses[ing the] technical capacities to monitor [information and communications technologies] ICT networks for early detection of threats"[24] a must and designated "limited incident detection and response capabilities [... as] a cause for concern"[25] (for other examples of relevant statements see Annex I).

Second, as a side effect, international cooperation on building detection capabilities also bears great potential for **building confidence** among donor and partner countries. This stems from exchanging experiences and leveraging synergies to address common challenges pertaining to a shared threat landscape (see further, Section 8.2).

Third, decision-makers may be interested in implementing measures aimed at building detection capabilities in other states by viewing this as a **strategic tool** to contribute to their own and collective security amidst competing geopolitical visions. As Pawlak put it: "donors increasingly view cyber capacity building projects not only as means to address the needs and improve [the] security of their partners but also as an investment in promotion of their own preferred vision of cyberspace."[26] Detection capability-building appears to be a good use case since donor countries are likely to be highly interested in enhancing detection capabilities in selected states especially when both face the same threat actors in their networks. For instance, the UK has been particularly outspoken in this regard, framing detection as an enabler of the disruption and deterrence of adversaries[27] and expressing its "committ[ment] to building our collective resilience to detect, disrupt and deter state and non-state threats around the world."[28] In a similar vein, the EU's 2025 International Digital Strategy emphasizes that "strengthening cybersecurity and cyber defence [of partner countries], including the capacity to detect, prepare for and respon[d] to cybersecurity threats and incidents, [...] is a direct investment in the EU's own security."[29]

Fourth, since situational awareness is the basis of any type of political response to cyber operations,[30] improved detection capabilities can **support not only the**

24 South African Representative (2024): Statement at 8th meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – Seventh Substantive Session.

25 South African Representative (2021): Statement at 4th plenary meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – First Substantive Session.

26 Patryk Pawlak (2016): Capacity Building in Cyberspace as an Instrument of Foreign Policy, Global Policy 7(1).

27 UK Government (2022): National Cyber Strategy 2022.

28 UK Foreign, Commonwealth and Development Office (2023): UNODA ICT Mapping Exercise: Contribution from the United Kingdom of Great Britain and Northern Ireland.

29 European Commission (2025): An International Digital Strategy for the European Union.

30 Sven Herpig (2021): Die Beantwortung von staatlich-verantworteten Cyberoperationen.

identification of "irresponsible" activities but also contribute to their attribution to specific threat actors or states. When this information is shared publicly or privately, it can help hold states accountable through diplomatic processes for not following the agreed dos and don'ts for responsible state behavior in cyberspace.[31] Developing more advanced detection capabilities also has the side effect of increasing the chance of detection, which may influence other states' cost–benefit calculus when deciding whether to engage in behavior that contravenes norms.

Lastly, detection capabilities are a key enabler in implementing UN cyber norms.[32] Hence, enhancing detection capabilities also has the side effect of **accelerating a partner country's ability to comply with UN cyber norms**. Of the 11 UN cyber norms, nine are closely associated with detection capabilities (see also Annex II).[33]

31 Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations: State of Play and Policy Options.

32 These norms are politically binding rules to guide state behaviour specifying do's and don'ts for the use of ICTs by states. In 2015, UN Member States agreed on a set of eleven norms for responsible state behavior in cyberspace, United Nations (2015): Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). Drawing from the report, the norms are usually alphabetized, starting with norm (a) and concluding with norm (k). For example, the U.S. has in the past explicitly sought to "promote the adoption of norms of responsible state behavior in cyberspace" through measures of foreign assistance, U.S. Department of State (n.d.): Cyber Capacity Building.

33 For some norms, there is a very clear and direct nexus between their content and detection capabilities, whereas for others, detection capabilities serve more as an auxiliary implementation factor. Detection capabilities are also listed among the capacities and steps contributing to implementation, as outlined in various documents, including relevant UN Group of Governmental Experts (GGE) guidance (United Nations (2021): Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135)), the most recent proposal of a UN norms implementation checklist by the UN OEWG II's Chair to be further discussed in the Global Mechanism (UN OEWG II Chairperson (2025): Draft Final Report of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021–2025, submitted to the 80th session of the General Assembly pursuant to General Assembly Resolution 75/240, Rev. 1), the ASEAN norms implementation checklist (ASEAN (2025): ASEAN Checklist for the Implementation of the Norms of Responsible State Behaviour in Cyberspace), and a relevant study by the UN Institute for Disarmament Research (UNIDIR, Samuele Dominioni and Giacomo Persi Paoli (2023): Unpacking Cyber Capacity-Building Needs: Part I. Mapping the Foundational Cyber Capabilities, UNIDIR). The OEWG II's Chair proposed Annex I was not adopted by states in the OEWG II's final report and therefore still remains a proposal at this stage. In the final report, UN Member States recommended to "continue discussing and updating, at the future permanent mechanism the Voluntary Checklist [...] with a view to its finalization," United Nations (2025): Developments in the field of information and telecommunications in the context of international security (A/80/257). For a full overview of the relevant passages of these documents, see Annex II.

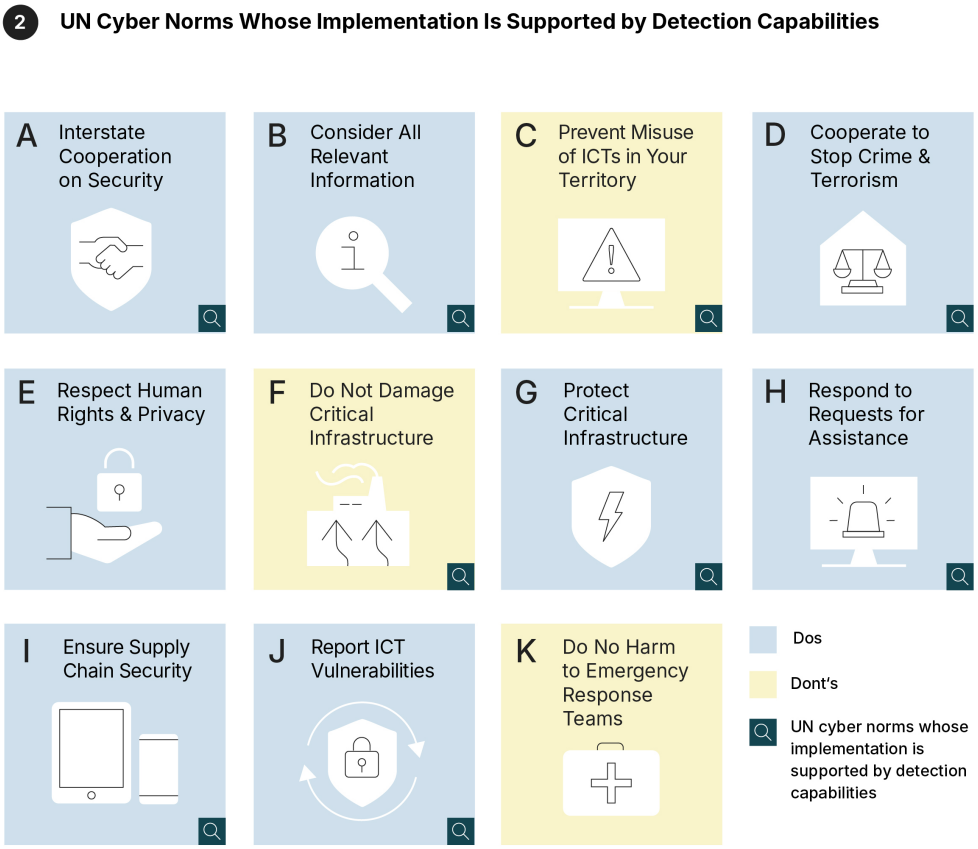


Figure 2: UN Cyber Norms Whose Implementation Is Supported by Detection Capabilities

By advancing detection capabilities, cyber diplomats can thus also **foster greater convergence on how international norms can be operationalized in practice.**[34] This, in turn, can make their implementation more tangible and contribute to building further political support. At a systemic level, this can help move UN discussions beyond the persistent debate over whether to prioritize the implementation of existing norms or the development of new ones, as it can facilitate dialogue on concrete steps governments can take to put the existing norms into effect.

The pop-out windows below explain how detection capabilities can support the implementation of each of the nine identified norms:

34 See also James Andrew Lewis (2020): Cyber Stability, Conflict Prevention, and Capacity Building, Center for Strategic & International Studies.

Norm A: "cooperat[ing] in developing and applying measures to increase stability and security in the use of ICTs and to prevent[ing] ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security"

Effective detection rests on cooperation within detection ecosystems. For instance, by facilitating information sharing, states can contribute not only to a shared perception of situational awareness but also to confidence-building among themselves. At the same time, an increased likelihood of detection can serve as one, albeit not necessarily the determinative, factor in a state's risk–benefit calculation of whether to engage in harmful ICT practices that may contribute to their prevention.

Norm B: "consider[ing] all relevant information" "in case of ICT incidents"

While response capabilities become central once an incident has been recognized, the incident's preceding detection is essential, as it enables an entity to collect *relevant information* in the first place. In other words, advanced detection capabilities increase the likelihood of recognizing an incident. They also facilitate capturing incident-specific and contextual data, which can contribute to a more comprehensive situational understanding during the response phase. This may also provide leads for further investigation and aid in attributing the identified operation or campaign to a specific threat actor or state on the basis of high-confidence evidence packs. Detecting malicious activity in one jurisdiction/network also enables detection in other jurisdictions/networks, which can support identifying and mitigating cascading effects across jurisdictions and critical infrastructure sectors.

Norm C: "not knowingly allow[ing] their territory to be used for internationally wrongful acts using ICTs"

Fulfilling this due diligence commitment requires states to identify internationally wrongful acts originating from their territory, which is something states can only do if they possess some form of detection capability themselves and maintain cooperative relationships with other actors, such as internet service providers (ISPs) and targeted entities, in their jurisdiction. Hence, before they can act on potential misuse, states must first be able to identify such actions themselves or be informed when others detect them. At the same time, and as noted in the 2021 GGE report, (non-)compliance with this norm is highly context-dependent due to varying national capabilities. Accordingly, the norm does not reflect a collective expectation that "states could or should monitor all ICT activities within their territory."[35]

35 United Nations (2021): Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135).

Norm D: "consider[ing] how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats"

To cooperate and exchange information on criminal or terrorist uses of ICTs, a government must first establish measures that enable the identification of such activities. This requires a clear understanding of what criminal or terrorist behavior—targeted against or committed through ICTs[36]—looks like in practice and how it can be recognized. It also involves knowing how to collect and retain relevant data, such as logs, that may serve as potential evidence and could be shared with international partners. Detection capabilities can enhance the extent and quality of evidence available to substantiate instances of criminal or terrorist use of ICTs, which also permits cross-border data correlation to identify common perpetrators or techniques and can advance further (joint) law enforcement actions.

Norm F: "not conduct[ing] or knowingly support[ing] ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"

Although this depends greatly on a state's threat visibility and its collaboration with other actors within its jurisdiction, states can monitor (at least parts of) outgoing network traffic. By doing so, they can identify whether some of their domestic infrastructure is being used to launch or relay *ICT activity contrary to their obligations under international law* against critical infrastructure abroad. However, compliance with this norm requires a comprehensive assessment drawing on multiple data sources, many of which cannot be obtained through detection alone.

Norm G: "tak[ing] appropriate measures to protect their critical infrastructure from ICT threats"

The norm continues as follows: "taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures."

Ongoing monitoring and analysis enables states to identify threats to vital sectors such as energy, healthcare, telecommunications, and transport before potential disruptions occur. The threat visibility provided by detection capabilities, along with lessons learned from previously detected incidents, can bolster preventive measures for safeguarding critical infrastructure (CI). Notably, detection capabilities, as defined and discussed in this paper, are also reflected in at least four of the eleven elements of the UN General Assembly resolution cited within the norm. The relevant elements include "facilitat[ing] the tracing of attacks on critical

36 Bundeskriminalamt (n.d.): Cybercrime.

information infrastructures and, where appropriate, the disclosure of tracing information to other States. [...]," [37] establishing emergency warning networks, and fostering public-private partnerships for information sharing and analysis.

Norm H: "respond[ing] to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts"

While assistance often focuses on limiting the spread and damage caused by particular incidents, detection capabilities can also help states respond to requests for support, either through established information-sharing arrangements or on an ad hoc basis. For example, detection-relevant support can be provided through the sharing of tactics, techniques and procedures (TTPs), indicators of compromise (IoCs) and knowledge exchange. This can help an affected state to assess the nature, scale, and impact of specific *malicious ICT acts.* Depending on how closely the requested and affected states are collaborating, requested states may also share high-level insights about similar issues found in their networks, which can support mitigation efforts.

Norm I: "tak[ing] reasonable steps to ensure the integrity of the supply chain"

Detection capabilities can enable states to identify compromised components, unauthorized modifications, or anomalous insertions in both software and hardware. Through continuous monitoring, states can detect unusual behavior after deployment and uncover vulnerabilities within software. These measures can support attaining the objectives outlined in the norm to enhance "end user [...] confidence in the security of ICT products" and to "prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions," as the detection of supply chain compromises enables taking *reasonable steps* to ensure their security.

For an overview of measures that governments can take to implement Norm I, see also Alexandra Paulus and Christina Rupp (2023): Government's Role in Increasing Software Supply Chain Security: A Toolbox for Policy Makers.

Norm J: "encourag[ing] responsible reporting of ICT vulnerabilities and shar[ing] associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"

By monitoring systems and networks for signs of anomalous behavior and acting as coordinators for (coordinated) vulnerability disclosure, states can identify and gain knowledge of actively exploited vulnerabilities, both within their jurisdictions and

---

37 United Nations (2004): Creation of a global culture of cybersecurity and the protection of critical information infrastructures (A/RES/58/199).

beyond. This situational awareness enables states to contribute meaningfully to structured vulnerability information-sharing processes both nationally and internationally, which in turn can help others detect—and thereby support "limit[ing] and possibly eliminat[ing]"—threats exploiting these vulnerabilities.

For an overview of measures that governments can take to implement Norm J, see also Sven Herpig (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action: How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace.

How to Build Governmental Detection Capability in Partner Countries: Responsibilities of Public Sector Entities

When discussing how to improve a country's ability to detect adverse events and incidents, it is important to first underscore the distinction between capabilities and capacities. In the context of a CSIRT's tasks, the Forum of Incident Response and Security Teams (FIRST) defines these terms as follows:[38]

Capability	Capacity
"A measurable activity that may be performed as part of an organization's roles and responsibilities"	*"The number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion"*

Table 1: Terminology – Capability vs. Capacity

In line with this distinction, **detection capabilities encompass hardware- and software-based technical tools (technology), human expertise (people), and procedural mechanisms (processes)**[39] **to monitor and analyze cybersecurity events—"any observable occurrence[s] in a network or system"**[40] **—to identify**

38 FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

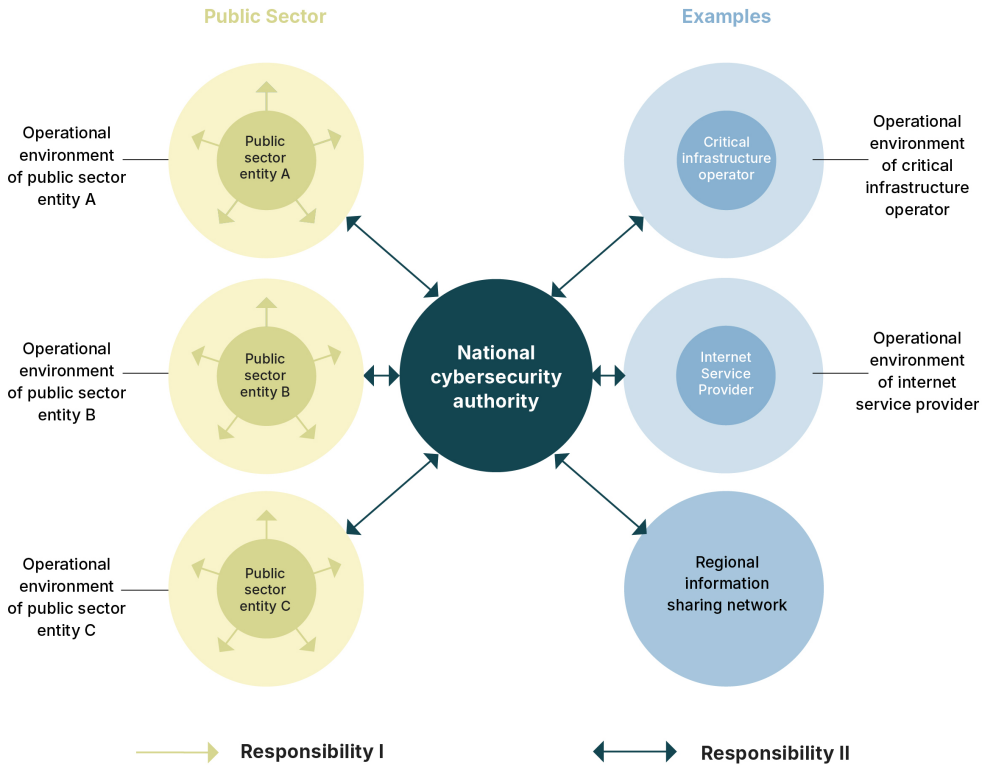
39 In addition to technology, people, and processes, a comprehensive detection capability also relies on physical assets, such as monitoring an entity's physical environment (International Organization for Standardization and International Electrotechnical Commission (2022): ISO/IEC 27002:2022) – for example, by "review[ing] and monitor[ing] physical access records" or "using alarm systems, cameras, and security guards," U.S. National Institute of Standards and Technology (2024): NIST CSF 2.0 Implementation Examples. Aspects pertaining to an entity's physical environment, such as these, are not within the scope of this paper.

40 National Institute of Standards and Technology (n.d.): Glossary - event.

unauthorized access attempts within designated IT environments.[41]

Building on the definition of detection capabilities and the FIRST differentiation, **international detection capability-building** involves helping partner countries or international organizations strengthen their technology, people, and process capabilities to monitor events and identify adverse cyber events and incidents. In contrast, detection capacity-building would entail improving and scaling already existing detection capabilities to, for example, cover more networks and infrastructures simultaneously. Despite the predominant reliance on the term cyber capacity-building (CCB),[42] this paper therefore intentionally employs the term detection capability-building.

3 Responsibilities of a Governmental Detection Capability



41 This scoping of detection capabilities draws on the Canadian Centre for Cyber Security's definition of detection as "the monitoring and analyzing of system events to identify unauthorized attempts to access system resources," Canadian Centre for Cyber Security (2020): Assemblyline.

42 Hakmeh, Swali, and Collett define cyber capacity-building as "an umbrella concept for various types of activity in which individuals, organizations and governments collaborate nationally or across borders to develop capacity and capabilities that mitigate cyber risks to the safe, secure and open use of information and communications technologies (ICTs)", Joyce Hakmeh, Amrit Swali and Robert Collett (2024): A principles-based approach to cyber capacity-building (CCB), Chatham House.

Figure 3: Responsibilities of a Governmental Detection Capability

In simplified terms, a governmental detection capability involves two core responsibilities that are carried out by different governmental entities within a national jurisdiction:

- **Responsibility I (see further Chapter 5): Implementing detection for their own operational environment** (akin, for example, to a ministry Chief Information Security Officer (CISO)'s responsibility). This responsibility necessitates having visibility into a government's and public sector's own systems paired with the ability to analyze this data. As such, **individual public sector entities**, such as governmental CSIRTs/SOCs of particular ministries, **need to put in place measures within their organization to monitor and analyze their own operational environment**. Subject to the level of financial investment and available in-house resources, these capabilities may be outsourced, in whole or in part, to be implemented by commercial external third parties, for example, through SOC-as-a-Service models (SOCaaS).
- **Responsibility II (see further Chapter 6): Advancing detection across the government and private infrastructure of a country** (akin to, for example, a national cybersecurity agency). This responsibility requires a country to undertake steps aimed at fostering a whole-of-nation approach to detection to enhance cross-entity coordination. In this regard, a **centralized entity with a nation-wide mandate**, such as a national cybersecurity authority (NCA) or national CSIRT, can **play a fundamental role in strengthening a nation's domestic and international detection ecosystems**. This is important because effectively detecting potentially adverse events across a nation is not an isolated activity. Effective detection depends on engagement and collaboration across a wide range of actors. Hence, a multi-stakeholder approach[43] is essential, not only because coordinated action strengthens the overall resilience of the ecosystem, but also because much of the relevant data such as cyber threat intelligence (CTI) often lies outside the direct reach of governments (e.g., with private entities such as ISPs).

This distinction between entities is important because these different actors not only have distinct responsibilities but also different levers at their disposal when it comes to carrying out these functions, which in turn shape the measures and activities that can be implemented to develop or enhance their capabilities.

Donor governments can use these distinct responsibilities as potential fields of action to make a tangible impact on the ground. They can further support assessment efforts by first evaluating a country's detection maturity. Such an assessment can involve examining which specific measures outlined in the

43 The importance of practicing multi-stakeholder cooperation in the area of threat detection was also underscored by several states in discussions within the most recent UN working group discussing cybersecurity matters, the UN Open-ended Working Group on security of and in the use of information and communications technologies (UN OEWG). For example, the EU pointed to the "active role [of non-governmental stakeholders] in threat detection" (European Union Representative (2023): Statement at 3rd meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – Sixth Substantive Session), Kazakhstan highlighted the benefits of public-private partnerships in facilitating effective detection (Kazakh Representative (2023): Statement at 6th meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – Sixth Substantive Session), Ghana stressed the great potential for collaboration with stakeholders to advance "cutting-edge cybersecurity solutions, especially in the areas of threat detection [...]" (Ghanaian Representative (2025): Statement at 2nd meeting, Open-ended working group on security of and in the use of information and communications technologies 2021–2025 – Tenth Substantive Session), and similarly Israel noted that "encouraging research initiatives in both public and private sectors can lead to breakthroughs in [...] threat detection" (Israeli Representative (2024): Statement at Global Round Table on ICT Security Capacity Building).

subsequent chapters are already in place and at what level of implementation. It also permits identifying gaps in the current situation, such as missing policies, (legal) frameworks, or organizational structures that are needed to ensure effective and sustainable governance. Based on this understanding, funders and beneficiaries can collectively define cyber-related development goals and design (an) appropriate intervention logic(s)[44] to guide targeted activities aimed at establishing or strengthening detection capabilities.

Importantly, it should be noted that both developing and enhancing detection capabilities is not a one-time effort. Since maintaining pace with threat actors (see also Section 8.2) requires continuously advancing capabilities, there is never a definitive "finish line." This requires strategic long-term patience and continuous investment in strategy, people, and tools—as this is also the case for already well-resourced countries with mature cybersecurity capabilities.[45]

Capabilities For Fulfilling Responsibility I: Detecting Adverse Cybersecurity Events

To find and analyze possible compromises within their operational environment, public sector entities need to put in place measures aimed at detecting adverse behavior. An entity's operational environment includes all assets, systems, services, interfaces, and environments used for information processing, including on-premise systems, networks, and cloud-based infrastructure.

Monitoring this environment includes collecting and analyzing endpoint and network-level data for holistic visibility. This can cover information such as who logs in at what time from where, what programs are opened, whether anyone tries to change important system settings, and what happens among systems and how they communicate within and beyond an entity's operational environment.

The U.S. National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) includes detection as one of its six core functions.[46] Specifically, the CSF lists two task categories for carrying out the "detect function":

44 These two steps relate to the design stages of identification and formulation in the EU's intervention cycle as outlined in Nayia Barmpaliou and Patryk Pawlak (2023): Operational Guidance: The EU's International Cooperation on Cyber Capacity Building, Second edition, EU CyberNet.

45 For example, the 2016 CMM review of the United Kingdom stated the following: "CERT-UK also performs incident response exercises, but the capacity for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities and a zero-level incident alert will not be met for some years," Global Cyber Security Capacity Centre (2016): Cybersecurity Capacity Review of the United Kingdom.

46 National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0.

Continuous Monitoring	Adverse Event Analysis
"Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events."	*"Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents."*

Table 2: Components of the "Detect Function" in the NIST CSF

As the NIST CSF does not consider the six functions in isolation—and since detection can contribute significantly to the response, recovery, and protection pillars as alluded to in the introduction—effective monitoring and analysis often require and rest on preparatory groundwork. Much of this groundwork falls under the NIST CSF's "govern" and "identify" functions, which act as enablers for the successful development and delivery of other functions.

Against this backdrop, the following sections outline selected measures[47] that can enable public sector entities to detect adverse events within their operational environment from three angles:

1. The **organizational context and operating framework** in place (Section 5.1);
2. The **measures to ensure continuous monitoring of its operational environment** (Section 5.2); and
3. The **foundations for analyzing adverse events occurring within their operational environment** (Section 5.3).

The measures outlined are not exhaustive but can serve as a foundational baseline, offering inspiration for potential efforts in partner countries, particularly where public sector detection maturity remains at lower levels. They are not intended to be prescriptive. Rather, each public sector entity must determine how best to ensure continuous monitoring and analysis of adverse events within its operational environment. This requires thoughtful consideration of key factors such as the entity's most critical assets, the tools that can be acquired, potential limitations in this regard, available funding, and the internal talent and resources that can be leveraged. Approaches will therefore naturally vary, and additional or different measures may be necessary depending on factors such as existing capabilities, the specific tactics, techniques and procedures (TTPs) of threat actors targeting the entity or country, as well as emerging technological developments.

47 While many of the measures presented in the following are also reflected in non-detection-specific standards such as the previously mentioned CSF framework or relevant ISO standards, this chapter takes a detection capability-specific perspective to highlight relevant elements with a focus on explaining how they relate and interact in one place.

Figure 4: Capabilities For Fulfilling Responsibility I: Detecting Adverse Cybersecurity Events

Organizational Context and Operating Framework

Summary

To build effective detection capabilities and manage the large volume of data relevant for detection, entities should establish foundational policies that support both implementation and operational effectiveness. This includes clearly **defining roles and**

responsibilities on the basis of a clear understanding of event monitoring and analysis. Foundational policies also include implementing a **logging policy** that, inter alia, identifies data sources, specifies which sources should be logged, and determines how long logs should be retained for basic threat detection and forensic capabilities. It can be equally important for entities to develop **guidance for triaging alerts**, maintain **channels and procedures for reporting**, and implement a **feedback loop** from these processes to improve detections and provide more valuable alerts over time. In addition, entities should leverage interdependencies and synergies with other fundamental measures such as maintaining an up-to-date **asset inventory**, conducting **risk assessments** to guide monitoring priorities and contextualize analysis, or raising **employee awareness** to notice unusual or suspicious behavior.

To build effective detection capabilities, an entity should have several foundational policies in place to support both their effectiveness and planned implementation.

Governance

Most importantly, an entity should have a **clear distribution of responsibilities** throughout the entire process laying out who does what and when.[48] For example, this includes which functional areas of the entity and which persons are responsible for operating and auditing relevant logging and analysis infrastructures, who configures the log sources, and who uses detection-related infrastructures and for what purpose to achieve well-defined interfaces between functional areas.[49] Depending on the entity's internal structure, these tasks may, for example, involve functional areas such as IT security operations, IT administration, information security management, auditing, and, where applicable, the entity's user help desk.[50]

Logging policy

Putting in place a comprehensive logging policy is essential for effective monitoring and, ultimately, for supporting incident response activities. Such policies lay the foundation for subsequent steps and measures aimed at detecting potentially adverse events within an entity's IT environment. Given the large volume of log[51] data generated within their networks, entities must establish processes to manage and

48 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

49 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

50 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

51 A log is "a record of the events occurring within an organization's systems and network," National Institute of Standards and Technology (n.d.): Glossary - Log. "Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network," Executive Office of the President (2025): Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity.

analyze this data effectively.

In developing a robust logging policy, an entity should consider the following:

- Determine the **applicable legal and contractual parameters** relevant to the entity's detection capabilities, as these may influence or stipulate what data can be collected, how it is evaluated, or how long it may be retained;[52]
- Identify data sources that produce valuable information for detection purposes and clearly define which **sources** are **to be logged** where in the entity's operational environment;[53]
- Specify **retention periods for logs** that comply with any applicable legal and contractual requirements, also taking into account the organization's risk profile[54] and ensuring logs are deleted once the defined retention period has elapsed;[55]
- Designate the **information to be recorded by each log**, for example, accounting for "the date and time of the event, the relevant user or process, the relevant filename, the event description, and the information technology equipment involved;"[56]
- Indicate which **event logging facilities** are being used and how logs are to be **transferred to a central logging infrastructure** (see further Section 5.2);[57] and
- Consider "any **shared responsibilities between service providers and the organization.**"[58] For example, if the entity has outsourced parts of IT infrastructure, it must ensure that the defined detection-related minimum baseline requirements are met by the relevant service providers.[59]

52 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen and Bundesamt für Sicherheit in der Informationstechnik (2023): DER.1 Detektion von sicherheitsrelevanten Ereignissen. For example, relevant legal parameters for an entity's logging policy may stem from national data protection laws or personality rights.

53 As a general guideline, the German BSI recommends that the decision on which log sources to monitor should be based on the entity's required level of protection: the higher the required level, the more events an entity should log, Bundesamt für Sicherheit in der Informationstechnik (2023): OPS.1.1.5 Protokollierung. An entity should also ensure that its logging infrastructure records not only security-relevant but also general operational events that may indicate a malfunction. For an overview of possible data sources, see MITRE (n.d.): Data Sources. At the system level, logs may, for instance, stem from firmware such as BIOS, virtual machines, operating systems, or system services, whereas logs from network components and traffic can, for example, be created by analyzing traffic amounts, bytes sent and received, data flows, routing data, or web server data, Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

54 UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C1 Security monitoring and Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection. NIST defines log retention as "archiving logs on a regular basis as part of standard operational activities," National Institute of Standards and Technology (n.d.): Glossary - Log Retention. In its guideline, the ACSC and its international co-authoring agencies recommend organisations to "retain logs for long enough to support security incident investigations [as] default log retention periods are often insufficient", especially when it comes to determining and responding to particular incidents. They also point to the challenge that insufficient data storage may pose to retaining logs and, in this respect, advise organisations to "implement data tiering such as hot and cold storage." For more information on data tiering, see, for example, SAP (n.d.): Data Tiering. For example, for security-relevant logs, the Australian Cyber Security Centre (ACSC) recommends to "retain[... event logs] in a searchable manner for at least 12 months," Australian Cyber Security Centre (2025): Guidelines for system monitoring.

55 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

56 Australian Cyber Security Centre (2025): Guidelines for system monitoring. Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection also provides examples – based on Executive Office of the President, Office of Management and Budget (2021): Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents – for possible event log details to be captured by entities.

57 Australian Cyber Security Centre (2025): Guidelines for system monitoring and Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen. The utility of a central logging infrastructure can be maximized if logs are "captured and stored in a consistent and structured format," Australian Cyber Security Centre (2025): Guidelines for system monitoring.

58 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection.

59 See also Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen. The German BSI also recommends entities to specify all logging and detection-related aspects in the context of external service provision in writing.

An entity should treat its logging policy as a living document, regularly reviewing its implementation and updating it to reflect any significant changes in its IT environment.[60]

Guidance, thresholds, and reporting channels

In addition to a logging policy, once it has been decided what is monitored and how, it is equally important to develop guidance on triaging alerts during the analysis stage,[61] to establish thresholds for security-relevant events, and to put in place and regularly test the channels and structures for reporting them.[62] For example, an entity may leverage tabletop exercises. In this regard the FIRST CSIRT Services Framework notes: "Instructions for analyst triage, qualification, and correlation need to be developed, for example in the form of playbooks and Standard Operating Procedures (SOPs)."[63]

Evaluation

In addition to planning and implementing measures aimed at detecting potentially adverse events, entities should also evaluate the effectiveness of these measures and incorporate lessons learned from their operation. A **continuous feedback loop** from triage and incident escalation (see Section 5.3)—which, among other things, links detection-related findings to prevention controls and analyst tuning—can strengthen an entity's overall detection posture. This feedback informs refining detection logics and processes, which can contribute to more valuable alerts over time. Ideally, this can also help prevent incidents similar to those successfully detected in the past and reduce false positives over time.[64]

Interdependencies with other fundamental measures

Because an entity's detection capabilities rely on its overall cybersecurity posture and thus the interplay with other functions of the CSF, there are various activities an entity can undertake that enhance its overall cyber resilience while fostering an

60 Bundesamt für Sicherheit in der Informationstechnik (2023): DER.1 Detektion von sicherheitsrelevanten Ereignissen and Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

61 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection practices. Such guidance, may, for example, include targeted information on "which log sources to examine, which systems to investigate and who to contact."

62 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

63 FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

64 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection practices and Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen. See also FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

environment in which its detection efforts can succeed. Importantly, the insights generated can also inform decisions on the technical tools, processes, and expertise required to achieve comprehensive monitoring and analysis, as outlined in the subsequent sections.

A few examples:

Maintaining a comprehensive and up-to-date **inventory of an entity's assets**[65] can aid an entity in developing policies on logging and detection by helping it understand the extent of its monitoring coverage, which can support "eliminat[ing] blind spots and gaps in coverage."[66]

To determine where an entity should focus its detection efforts (e.g. which sources to monitor first under resource constraints), it is also useful for an entity to prioritize based on (at least) two factors: importance and risk. This requires **understanding how critical specific networks, systems, and information are to the entity**.[67] It also involves identifying and evaluating risks to the entity through a **risk assessment**.[68] For example, a risk assessment can help determine the extent of coverage needed based on the entity's required level of protection. A continuously updated **threat profile** that informs the risk assessment can further identify specific threats to enable risk prioritization.

Complementary to measures aimed at monitoring at the technical level (see Section 5.2), raising **employee awareness** can have a positive impact on an entity's detection posture. Since employees are system and network users, they are often well-positioned to notice unusual or suspicious behavior in their daily work.[69] To leverage this, entities should invest in continuous security awareness training to help employees become more sensitized and vigilant to potential threats. Simultaneously, to ensure that any employee observations contribute effectively to detection efforts, it is important to have clear procedures in place for reporting such irregularities or suspicions to appropriate internal channels.

65 For example, National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0 and FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

66 Microsoft (n.d.): What is a security operations center (SOC)?.

67 For example, MITRE (2024): Crown Jewels Analysis and U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Secure High Value Assets (HVAs).

68 For example, National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0 and Dutch National Cyber Security Centre (2017): Factsheet Building a SOC: start small.

69 For example, employee awareness-raising is considered a 'must' in the logging and detection minimum baseline standard of Germany's BSI, Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

Monitoring

Summary

Monitoring requires capturing and aggregating all relevant activity across a public sector entity's operational environment. This, inter alia, involves **configuring IT systems and applications** to log security-relevant events and usually necessitates **implementing additional tools**, such as EDR or intrusion detection systems (IDS), to achieve full coverage. Entities should consider using a **centralized data management system**, such as a data lake or a Security Information and Event Management (SIEM) system, to collect and aggregate this information, enabling tools and human analysts to subsequently systematically view, filter, and analyze events across the entire environment.

After outlining a general logging policy, an entity's focus should shift to the actual collection of logs and their subsequent management. The term log management refers to the "process for generating, transmitting, storing, analyzing, and disposing of log data."[70] Log collection refers to the process of automatically transferring events to be logged to a central logging infrastructure and storing them there.[71] The analysis of log data will be addressed separately in Section 5.3.

Log collection

In the log collection stage, an entity should ensure that all data sources identified during the logging policy stage are covered, providing full visibility into these sources.[72] The type of log source determines both what kind of data an entity can collect for monitoring and how that data can be collected.

To collect this information, an entity should **configure IT systems and applications** within its operational environment to log all security-relevant events[73] with regular reviews to ensure that logging is functioning as intended. An entity should also consider **integrating additional tools** to guarantee the logging of general and

70 National Institute of Standards and Technology (n.d.): Glossary - Log Management.

71 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

72 As minimum log sources to consider for active monitoring, the UK National Cyber Security Centre (NCSC) lists the following categories and non-exhaustive examples: (1) website traffic going to the internet, (2) email traffic, (3) IP connections between an entity's network and the internet, (4) if applicable, IP connections between zones in operational technology (OT) networks, and (5) host-based activity, UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C1 Security monitoring. At the system level, the German BSI recommends logging, at a minimum, data related to activities such as the creation and modification of permissions and users, changes to access credentials, successful and failed login attempts, execution of applications, and installations, among other examples of activities, Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

73 To that end, entities should also leverage logging functions embedded in many operating systems or applications, which are either already included or can be integrated through the use of additional products, Bundesamt für Sicherheit in der Informationstechnik (2023): OPS.1.1.5 Protokollierung.

security-relevant logs from the network perspective and achieve the intended level of coverage as specified in an entity's logging policy.

To gather the relevant telemetry, an entity has various tools at its disposal, including Domain Name System (DNS) logging tools,[74] tools for collecting network flow data (NetFlow tools),[75] malware and vulnerability scanners, antivirus software, intrusion detection systems (IDS),[76] endpoint monitoring systems such as EDR[77] solutions, or cloud detection tooling such as cloud security posture management (CSPM).[78] Some of these tools also have built-in analytical capabilities that automatically trigger alerts for further analysis (which will be further discussed in Section 5.3).

Log management

Once processes and technical measures have been implemented to collect logs across an entity's infrastructure, it is essential to ensure their proper management. This requires a **centralized log management infrastructure** to which the designated systems and implemented tools can automatically feed their log data.[79] The central goal at this stage is **log aggregation** to enable effective log analysis in a subsequent step. Maintaining a centralized log repository is essential, as only such a repository allows analysts to view, filter, and systematically analyze log data.[80] This is especially important, since indications of malicious activity are "rarely [...] isolated events on a single system component or system."[81]

74 For example, "Passive DNS (PDNS) systems gather information about DNS records in particular time points, in order to provide historical information about such records. The systems help in tracking changes of malicious infrastructure in time, but also provide last known IP address of a domain if the DNS record is no longer available" or "DNS request monitoring systems provide information about how often and when certain domain names were queried and by which addresses. Thanks to that, extended analyses can be performed, including popularity of domains, their activity lifetime, but also tracking of botnet clients when monitoring known [command and control] C&C domains," ENISA (2020): Measures for proactive detection of incidents, GitHub.

75 "Network flow monitoring systems provide means for extraction of network flow information from network traffic. Some of the systems also help in basic analysis of network flows, including bandwidth level, protocol usage and IP addresses involved in communication," ENISA (2020): Measures for proactive detection of incidents, GitHub.

76 An IDS "is a tool that detects security-relevant events on a system or network basis and helps to evaluate, escalate and document them. Security-relevant events can be detected based on patterns and/or anomalies". One can distinguish between host-based IDS and network-based IDS (NIDS). NIDS "monitors the network traffic on one or more network segments for security-relevant events. IDS functionality is usually integrated in firewalls at network transitions. IDS sensors are typically used within individual network segments and monitor the network traffic at central switches via mirror ports or individual network connections via inline [Test Access Points] TAPs," whereas a host-based IDS "runs on the systems to be monitored [... and is] typically used to detect security-relevant events at the application or operating system level," Bundesamt für Sicherheit in der Informationstechnik (2022): Orientation Guide to Using Intrusion Detection Systems (IDS). A TAP is "a device used to monitor and analyze network traffic without disrupting the normal operation of the network. It is typically placed between two Ethernet devices and operates transparently, allowing it to capture and mirror all the data passing through the connection," Hilscher (n.d.): Test Access Point (TAP).

77 "The term "endpoint detection and response" means cybersecurity tools and capabilities that combine real-time continuous monitoring and collection of endpoint data (for example, networked computing device such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities," Executive Office of the President (2025): Executive Order 14144: Strengthening and Promoting Innovation in the Nation's Cybersecurity.

78 "Cloud security posture management (CSPM) is the process of monitoring cloud-based systems and infrastructures for risks and misconfigurations," Microsoft (n.d.): What is CSPM?.

79 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

80 Bundesamt für Sicherheit in der Informationstechnik (2023): OPS.1.1.5 Protokollierung.

81 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection practices.

There are various tools differing in scope and sophistication available to enable centralized log aggregation and management.[82] The predominant tool used is a **Security Information and Event Management (SIEM) system**,[83] which integrates log collection as one component of a more comprehensive solution for security monitoring and analysis.[84] Logs should be forwarded to the entity's centralized logging infrastructure in near real time to enable the timely detection of suspicious activity and reduce response latency.[85]

In initiating and maintaining a centralized logging infrastructure, an entity should consider various factors:

- **Sizing the infrastructure** in such a way that the logged events could be retained for twice the duration of the identified retention period;[86]
- Ensuring **event log backups** and implementing "**data redundancy practices**;"[87]
- **Protecting event logs during transit and at rest**;[88]
- Providing for and monitoring restrictive access[89] to the infrastructure and putting in place **technical safeguards against unauthorized access, tampering, or uncontrolled deletion of log data**;[90] and
- Continuously **monitoring the logging infrastructure for error conditions**.[91]

82 For some tools, this functionality is embedded as part of one of the tools activities and functions, while for others, it represents their primary purpose. On log centralisation vs. log analysis see also Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: practitioner guidance.

83 Agencies from the Five Eye countries as well as Czechia, Japan, Singapore, and South Korea define a SIEM as described below, with most of the identified features being relevant for log analysis as discussed further in the analysis section: "a type of software platform or appliance that collects, centralises, and analyses log data from sources within a network or system for the purpose of cyber security. If properly implemented for this purpose, a SIEM platform automates the collection and centralisation of important log data that would otherwise be scattered across a network, thus making it easier for a human security team to navigate. Unlike some other log collection and centralisation tools, a well-configured SIEM then applies a predefined baseline of business-as-usual network activity, rules and filters to analyse and correlate the log data. This analysis can allow the SIEM platform to detect unusual activity on the network, which may represent a cyber security event or incident. Most SIEM products enhance their analysis by incorporating up-to-date threat intelligence," Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: practitioner guidance.

84 A different example would be a secured data lake which is primarily designed for centralized log storage, Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: practitioner guidance.

85 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection and Australian Cyber Security Centre (2025): Guidelines for system monitoring.

86 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen. The German BSI justifies its recommendation for a doubled duration by noting that the complexity of modern information networks and diverse attack scenarios is expected to increase logging volumes. For example, for security-relevant logs, the Australian Cyber Security Centre (ACSC) recommends entities to "retain[… event logs] in a searchable manner for at least 12 months," Australian Cyber Security Centre (2025): Guidelines for system monitoring.

87 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection.

88 For example, in this respect, ACSC and its co-authoring entities recommend "implement[ing] secure mechanisms such as Transport Layer Security (TLS) 1.3 and methods of cryptographic verification", Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection. See also Australian Cyber Security Centre (2025): Guidelines for system monitoring and Bundesamt für Sicherheit in der Informationstechnik (2023): OPS.1.1.5 Protokollierung.

89 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

90 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection, Bundesamt für Sicherheit in der Informationstechnik (2023): OPS.1.1.5 Protokollierung and UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C1 Security monitoring. The German BSI also encourages entities to ensure that administrators themselves do not have the authorization to alter or delete the recorded logging data. With a view to the threat landscape, taking measures in this regard is also particularly important since threat actors are known to attempt "modify[ing] or delet[ing] event logs to hide their tracks," see further, for example, U.S. Cybersecurity and Infrastructure Security Agency (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

91 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

Ideally, the infrastructure should be operated in a physically segmented network zone with enhanced security controls given its high attractiveness to threat actors and potential to become a "single point of failure in an organization's detection capability."[92] However, it should be noted that this element is less feasible for entities that have outsourced (parts of) their incident management. For example, in managed service contexts or cloud computing environments such physical segmentation no longer exists in the same form. Where segmentation is not (or not yet) feasible, other options such as cloud-based log aggregation can serve as interim solutions.

Moreover, given the variation in log structure, an entity should also determine whether **enriching or normalizing log data** is required to enable their subsequent analysis as this can enhance consistency and improve correlation.[93]

Analysis

Summary

Given the vast volume of (log) data generated, manual analysis should be reserved for prioritized alerts while **automated tools** continuously evaluate collected data with the objective of generating alerts for potentially adverse events. Tools like SIEM can **compare system and network data against metrics such as vendor-provided rulesets, CTI, normal activity baselines, or custom detection logic** to identify anomalies and reduce the total number of security-relevant events. Using this information to filter, enrich, and correlate information can help guide both automated tools and human analysts in **distinguishing legitimate from suspicious activity**. Once alerts have been triggered, entities need to qualify true positives from false alarms. This step can not only initiate the response process but also generate analytical insights that can improve the entity's preventive and detection efforts.

Following the collection and aggregation of log data, it is even more important to implement measures aimed at their analysis, defined as the "study[... of] log entries to identify events of interest or suppress log entries for insignificant events."[94] Whereas monitoring aims to identify anomalies in the first place, analysis focuses on interpreting and making sense of the detected irregularities.

92 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection and Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

93 An entity may do so, for example, by mandating a specific log format or by implementing automated log normalization methods, National Institute of Standards and Technology (n.d.): Glossary - Log Normalization, Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection and Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen. For more information on log normalization, see, for example, Splunk (2024): Data Normalization Explained: An In-Depth Guide.

94 National Institute of Standards and Technology (n.d.): Glossary - Log Analysis.

Tools

It is essential for entities to incorporate **automated analysis tools** that continuously evaluate the collected data. The tools that an entity can use for that purpose vary in sophistication as they have the ability to "apply a range of methods, from simple logic or pattern-matching rules to the application of statistical models or machine learning."[95] When selecting tools, entities should consider both the requirements for using AI-powered software and the potential security implications of open-source tools. Careful tool selection, proper integration into an entity's detection posture, and knowledge of potential risks are essential in this respect. In cases where an automatic qualification of alerts is not possible, an entity must account for their manual analysis.[96]

Once logs have been aggregated in a centralized logging infrastructure, organizations should facilitate their analysis in a resource-efficient and -preserving manner. Given the vast volume of log data generated, manual analysis should not be the default option and should be reserved for selected, already prioritized alerts. To this end, the Australian Cyber Security Centre (ACSC) and some of its international counterparts recommend that entities "consider filtering [and selecting] event logs before sending them to a SIEM or [Extended Detection and Response] XDR[97] to ensure [the tool] is receiving the most valuable logs to minimise any additional costs or capacity issues."[98]

Tools like SIEM or XDR can then automatically **compare system and network data against a variety of metrics to detect anomalies** and potential threats. These metrics can be sourced externally (e.g. through "rulesets provided by the vendor [... which] should be updated regularly"[99]) or developed and maintained internally and tailored to a specific entity profile, provided the log analysis tool supports such as individualized configuration.[100]

The overarching goal at this stage is to have these automated tools **generate alerts for**

95 FIRST (2019): FIRST CSIRT Services Framework Version 2.1.

96 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

97 XDR is the abbreviation for 'extended detection and response.' "XDR is a software as a service tool that offers holistic, optimized security by integrating security products and data into simplified solutions. [...] In contrast to systems like endpoint detection and response (EDR), XDR broadens the scope of security, integrating protection across a wider range of products, including an organization's endpoints, servers, cloud applications, emails, and more. From there, XDR combines prevention, detection, investigation, and response to provide visibility, analytics, correlated incident alerts, and automated responses to improve data security and combat threats," Microsoft (n.d.): What is a security operations center (SOC)?.

98 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection.

99 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection.

100 As a general rule of thumb, the more configurable and customizable a log analysis tool is, the more expensive and resource-intensive it is likely to be to maintain, UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection.

potentially adverse events, such as when specific activities are detected to exceed particular predefined thresholds. These events are then collated, reviewed, and validated by human analysts. Those that exceed a predetermined severity threshold are escalated to incidents, which then trigger a response.

Measures that can guide both the tools' and human experts' analytical direction include the following, which will be discussed in greater detail in subsequent subsections:

- The collection and integration of **CTI** and other contextual information;
- The establishment and maintenance of a **baseline of acceptable normal activity**; and
- The development and upkeep of **detection logic** or **custom detection use cases**.

The analysis of adverse events can further benefit from an entity maintaining a risk assessment and threat profile, which help contextualize observed irregularities and assess event severity. Furthermore, an updated asset inventory can provide indications of the potential scope and degree of exposure.

CTI integration

To collect CTI, entity personnel can draw upon "open discussion forums, trusted relationships, paid-for contracts with threat intelligence companies or [internal] generat[ion]," [101] which can shed light, for example, on known **indicators of compromise** (IoCs), specific malware types, or new **TTPs**. [102] This step also involves continuously monitoring information on technical vulnerabilities and intrusion patterns related to the systems used by the entity, as well as determining their relevance for the entity's operational environment. Information sources include system manufacturers or national cybersecurity authorities (NCAs). [103] The UK NCSC recommends accounting for the possibility of automatic ingestion of CTI feeds in an entity's analytical detection infrastructure, which could be a SIEM. [104] If an entity maintains a threat profile, this can facilitate prioritizing the ingestion of CTI specific to the identified threats.

Baseline

A baseline comparison of what normal benign activity looks like within an

101 UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C1 Security monitoring.

102 In a 2020 study, the EU's cybersecurity agency ENISA listed information sources that entities can consult for the purpose of proactive detection, including, for example, feeds of malware URLs, phishing sites, or botnet command and control servers, European Union Agency for Cybersecurity (2020): Proactive detection – Measures and information sources. See also Otmar Lendl (2023): A classification of CTI Data feeds, CERT.at.

103 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

104 UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C1 Security monitoring.

organization's operational environment can support identifying and qualifying legitimate versus illegitimate signs of activity.[105] To develop and maintain such a baseline that helps with analyzing deviations (i.e., abnormalities) from the baseline, it is important that an entity has a "good **understanding of normal system behaviour** (e.g. what software is authorised and how it would normally behave, how user accounts normally access network resources or how network components connect to each other and transfer data)."[106] This also includes recognizing regular patterns and dependencies, such as day/night or weekend traffic, scheduled maintenance, and holiday periods.[107] An entity should ensure that it regularly assesses whether its baseline understanding requires recalibration and updates, such as when there are changes to the system or network perimeter or based on "current threat intelligence."[108]

Detection use cases and detection logic

Depending on an entity's individual risk profile, it should be taken into consideration that, when using commercial tools, "detection is biased towards techniques that benefit the widest range of customers."[109] As a result, global vendors' detection tools may be unable to reflect regional/local threat landscapes or sector-specific risks. To address this potential bias, public sector entities should consider whether they need to supplement commercial tools with **context-specific threat intelligence or detection rules tailored to their local threat landscape**. If an entity has an elevated risk profile or specific monitoring coverage requirements (e.g., through proprietary systems), it may also need to develop **custom detection use cases**[110] and techniques.[111] Doing so comes with various prerequisites in terms of

105 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection practices.

106 UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C2 Threat Hunting. A baseline "is derived by performing an analysis of normal behaviour of some user accounts and establishing 'always abnormal' conditions for those same accounts," Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection. Also, keeping an entity's asset inventory updated can complement a baseline assessment of normal system and network behavior.

107 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

108 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen and UK National Cyber Security Centre (2024): Cyber Assessment Framework - Principle C2 Threat Hunting.

109 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection.

110 FIRST defines a detection use case as a "specific condition to be detected by a [CSIRT's] Information Security Event Management service area," FIRST (2019): FIRST CSIRT Services Framework Version 2.1. Their CSIRT Services Framework further notes that "the terminology [of a use case] originates in software engineering, but is now widely used in detection engineering." For example, potential detection use cases could be "identify[ing] when high-risk users log in to machines infected with malware" or "look[ing] for compromised accounts by identifying geographically impossible logins," Splunk (n.d.): Identify the relevant use case for your detection in Splunk Enterprise Security. If use cases are employed, an entity needs to continuously evaluate each detection use case's "benefit/effort ratio" and, based on that assessment, adjust or discard the rationale underpinning the use case, FIRST (2019): FIRST CSIRT Services Framework Version 2.1. To test and improve detection use cases, an entity may carry out red or purple team exercises as a proactive way to search for threats, providing an avenue to strengthen its overall detection capabilities, UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection practices. As developing and maintaining detection use cases is a very resource-intensive endeavor and "to improve the detection capabilities for everyone," there are also related community-driven efforts an entity may consult and integrate in its analytical portfolio, such as the vendor-agnostic open source rule repository Sigma, SigmaHQ, GitHub.

111 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection.

resources, such as the configurability of tools and the availability of highly skilled personnel to develop and maintain detection rules.[112]

Correlation, triage, and qualification

Once there is an indication of a potential incident based on the collected logs and initial (automated) analysis, an entity must **distinguish between a real information security incident and a false alarm**. This process involves "identify[ing] events directly related to other potential or ongoing security incidents" by "grouping [...] related potential information security incidents for combined qualification or updating to an existing information security incident already handled" (correlation) and "triag[ing] and qualify[ing] detected potential information security incidents in order to identify, categorize, and prioritize true positives."[113]

If an entity maintains an in-house analytical capability, the triage of alerts and, if needed, their manual qualification requires highly specialized personnel.[114] Therefore, an entity should ensure that adequate budget is reserved for their continuous training, such as when new IT components are introduced into the entity's perimeter that could affect its overall detection posture.[115] To reduce "alert fatigue,"[116] organizations should consider implementing at least some form of automated triage,[117] enabling human analysts to concentrate on the most critical detected events in alignment with the organization's overall risk profile. Where automation is not yet feasible, basic manual triage guided by structured playbooks can still improve distinguishing true security threats from irrelevant or false alerts. Given the vast volume of log data that must be analyzed to make such decisions, the evolving development of AI-based tools offers considerable potential to assist entities in investigating alerts and providing guidance for determining whether they represent false alarms or true positives.

Detection capabilities and response automation: By way of an aside for the sake of completeness (although this already feeds into the response stage following a detected incident and is therefore not exclusively a mere detection capability) it should be noted that entities, depending on their required level of protection, may also (need to) use tools automating parts of a response,[118] such as Security Orchestration,

112 UK National Cyber Security Centre (2022): Building a Security Operations Centre (SOC) - Detection.
113 FIRST (2019): FIRST CSIRT Services Framework Version 2.1.
114 Bundesamt für Sicherheit in der Informationstechnik (2023): DER.1 Detektion von sicherheitsrelevanten Ereignissen.
115 Bundesamt für Sicherheit in der Informationstechnik (2023): DER.1 Detektion von sicherheitsrelevanten Ereignissen.
116 FIRST (2019): FIRST CSIRT Services Framework Version 2.1.
117 In this context, the FIRST CSIRT Services Framework notes that "mature tooling facilitates effective triage by enriching with context information, assigning risk scores based on the criticality of affected assets and identities and/or automatically identifying related information security events," FIRST (2019): FIRST CSIRT Services Framework Version 2.1.
118 Bundesamt für Sicherheit in der Informationstechnik (2023): DER.1 Detektion von sicherheitsrelevanten Ereignissen.

Automation, and Response (SOAR)[119] platforms. These tools automate not only parts of log data analysis—relevant to the detection of adverse cyber activities—but also aspects of response, for example "by applying predefined playbooks, which set certain actions to be taken when specific events occur, such as isolating the source of the event in the network."[120] There are also modern systems providing for the delivery of contextual containment.[121] Having such mechanisms in place can be important for initial containment, as it contributes to altering the ratio of damage done to damage potentially avoided. However, while automated response tools like SOAR platforms hold the potential to offer strong benefits, their effective use typically requires mature processes and skilled personnel.

Capabilities For Fulfilling Responsibility II: Fostering (Inter)National Detection Ecosystems

NCAs play a central role in building and advancing national and international detection ecosystems due to their mandate to oversee national cyber resilience and convene stakeholders across sectors. In the context of this paper, an NCA's institutional setup is treated as a black box, acknowledging that its structure, mandate, and resource level can vary significantly across countries depending on local circumstances. For the purpose of this discussion, it is simply assumed to hold a central coordinating role within a country's cybersecurity ecosystem. For example, an NCA may take the form of a national cybersecurity agency or a national CERT/CSIRT in states with the requisite capacity.[122]

NCAs can promote the development and adoption of detection tools and processes, support capacity building across public and private actors, and foster (platforms for) trusted information sharing and interoperability—all of which contribute to enhancing whole-of-nation situational awareness and preventing fragmentation. In practice, this requires an NCA to collaborate with multiple layers of target

119 Agencies from the Five Eye countries as well as Czechia, Japan, Singapore, and South Korea define a SOAR as "a type of software platform that builds upon the collection, centralisation, and analysis of log data. Some SOAR platforms perform these functions themselves, while others integrate with an existing SIEM and leverage its log collection, centralisation, and analysis. Either way, a SOAR automates some of the response to detected cyber security events and incidents. It does so by applying predefined 'playbooks', which set certain actions to be taken when specific events occur, such as isolating the source of the event in the network. These automated actions do not replace human incident responders but can complement them," Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: Executive guidance.

120 Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: Executive guidance.

121 For example, Darktrace (n.d.): Darktrace Autonomous Response: Keeping pace with evolving threats.

122 It should be noted, however, that the NCA's institutional placement, for example, within a country's Ministry of the Interior, Ministry of Justice, or intelligence services, can have profound implications for its ability to foster a detection ecosystem. This is because the NCA's institutional location can determine its level of visibility and influence its ability to build trusted relationships with a broad range of stakeholders. See also Hanneke Duijnhoven, Bram Poppink, Tom van Schie and Don Stikvoort (2021): Getting started with a national CSIRT.

audiences, both nationally and internationally:

- **Layer 1:** Relationships with **other public sector entities within their jurisdiction**, such as various government departments, entities administering unemployment benefits, law enforcement agencies, central banks, or municipalities and cities;
- **Layer 2:** Interactions with **non-governmental actors at the domestic level**, such as privately owned critical infrastructure operators, ISPs, the cybersecurity community or academia; and
- **Layer 3:** Collaboration with **other states and internationally operating stakeholders**, such as national cybersecurity entities in other states, multinational companies, regional or multilateral fora like CSIRT networks, or international non-governmental organizations such as FIRST and the Shadowserver Foundation.[123]

To achieve this, NCAs can leverage a range of tools and instruments to establish and nurture the interactions necessary for a robust detection ecosystem. The roles they undertake—and the extent to which they are exercised in practice—can vary significantly in nature, scope, and required capacity. For example, depending on the country in question, some functions undertaken by NCAs, like maintaining central threat intelligence-sharing platforms, may require substantial new investment in financial and human resources, while other functions can be performed as an expansion of existing functions. Others may arise from legal obligations, as is the case, for example, for EU Member States under the NIS 2 Directive, whereas some functions may be adopted voluntarily in pursuit of broader strategic or political objectives. In a similar vein, certain tasks may require a specific legal basis, as outlined in frameworks like the 2015 U.S. Cybersecurity Information Sharing Act.[124]

To illustrate the diversity of potential contributions by NCAs in furthering (inter)national detection ecosystem(s), this chapter outlines three activity areas:

1. **Monitoring and analysis** (Section 6.1);
2. **Information sharing and operational advice** (Section 6.2); and
3. **Operational, financial, and non-material assistance** (Section 6.3).

123 Disclaimer: This layer does not focus on international cooperation in the field of capacity-building. Examples of activities of that nature are examined in Chapter 7.

124 U.S. Congress (2015): An act to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes (Cybersecurity Information Sharing Act of 2015) and Michael Daniel (2025): The Case for Reauthorizing CISA 2015, Lawfare.

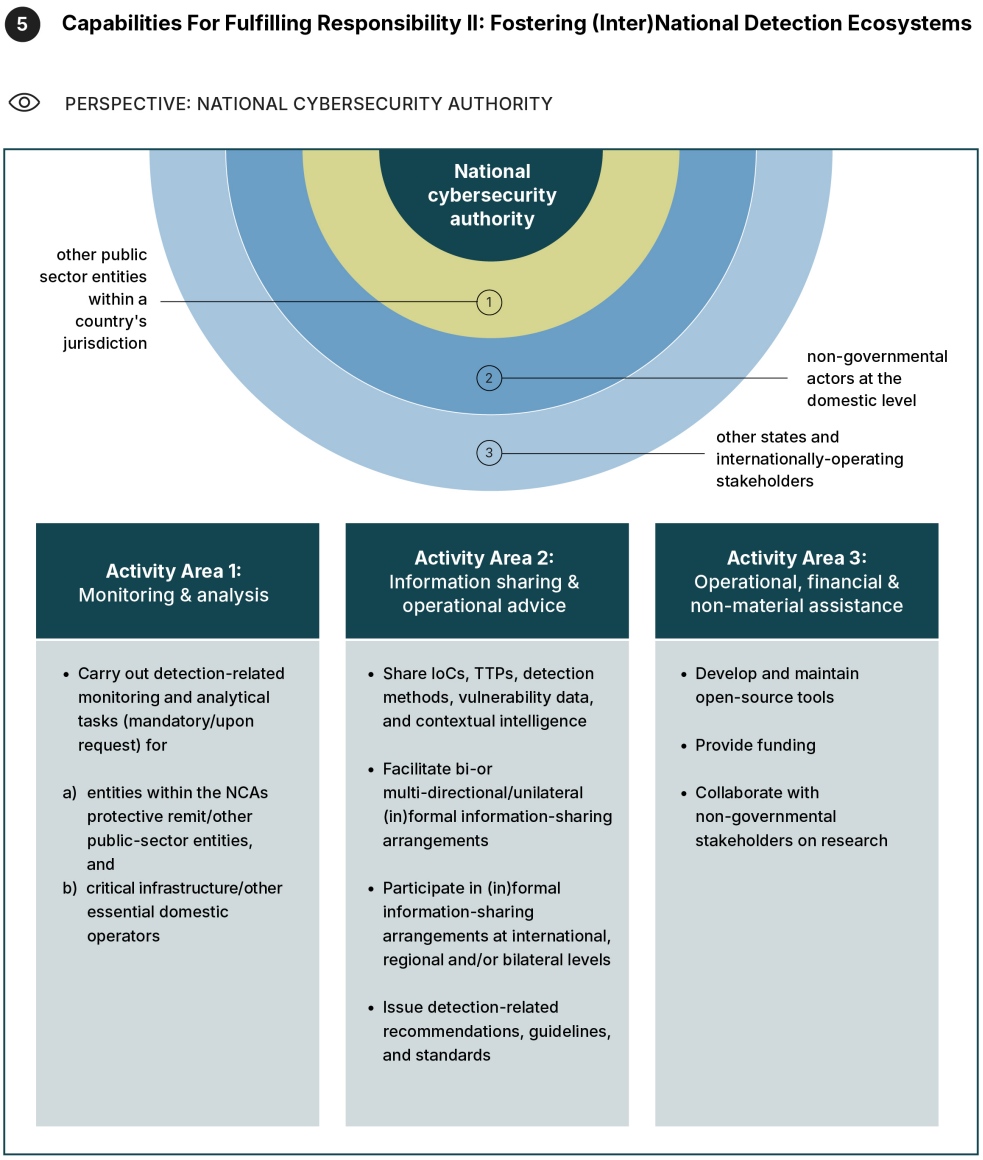


Figure 5: Capabilities For Fulfilling Responsibility II: Fostering (Inter)National Detection Ecosystems

In the following sections, each activity area will be explored via concrete examples of what could be done—and not necessarily what every NCA should be doing—highlighting this broader ecosystem in action. **An NCA's ability to fulfill these roles** requires not only technical capacity and legal authority but **ultimately hinges on its ability to build trust and credibility within the cybersecurity community**, making both formal and informal community-building essential enablers.

Monitoring and Analysis

In many jurisdictions, NCAs are directly responsible for protecting government systems and other public sector networks from malicious cyber activities. In the EU, the NIS 2 Directive also stipulates that the tasks of national CSIRTs comprise the "monitoring and analysing [of] cyber threats, vulnerabilities and incidents at national level" (Art. 11(3), point (a)).[125] Often, this protective mandate also involves carrying out detection-related analytical tasks for entities within an organization's protective remit and other public sector bodies. For example, this may include the monitoring network traffic of entities, collecting information on anomalous activity, or offering "detection-as-a-service" (DaaS), through which public sector entities can send their logging data to the NCA for analysis.

Three examples of programs implemented by existing NCAs are as follows:

United States: EINSTEIN/Cyber Analytics and Data System (CADS) – Layer 1

In 2003, then US-CERT within the U.S. Department of Homeland Security launched the so-called EINSTEIN capability, also known as the National Cybersecurity Protection System (NCPS), which is now integrated in the U.S. Cybersecurity and Infrastructure Security Agency (CISA). With the U.S. Federal Civilian Executive Branch (FCEB) as its exclusive target audience, EINSTEIN is "a sensor grid that monitors network traffic for malicious activity to and from participating departments and agencies."[126] Over the years, EINSTEIN capabilities were expanded to also encompass "signature-based and anomaly-based intrusion detection (IDS) capabilities" (EINSTEIN 2, 2008) and intrusion prevention (EINSTEIN 3, 2010),[127] yet these were discontinued in 2024. With advancing technological developments, EINSTEIN's limitations, such as its "reli[ance] on detecting known threats"[128] rather than "being able to identify novel malicious traffic at first encounter,"[129] as well as its "focus[...] on perimeter defense [... when] most enterprises no longer even have a perimeter to defend,"[130] led CISA to announce a new initiative, the Cyber Analytics and Data System (CADS) to replace EINSTEIN/ the NCPS[131].

125 Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 2022/2555.
126 U.S. Cybersecurity and Infrastructure Security Agency (n.d.): National Cybersecurity Protection System.
127 Andreas Kuehn (2013): Extending Cybersecurity, Securing Private Internet Infrastructure: The U.S. Einstein Program and its Implications for Internet Governance.
128 U.S. Congress (2023): Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs: Hearing Before the Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security, House of Representatives.
129 Chris Jaikaran (2023): DHS's Cybersecurity Mission—An Overview, Congressional Research Service.
130 U.S. Congress (2023): Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs: Hearing Before the Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security, House of Representatives.
131 U.S. Cybersecurity and Infrastructure Security Agency (2025): Cyber Analytic and Data System.

United Kingdom: Host Based Capability (HBC) – Layer 1

The UK NCSC maintains the Host Based Capability (HBC) service for UK central government entities with which it has established an agreement for HBC provision. These entities, who are selected on a "strategic case-by-case basis," can use the services of the HBC free of charge.[132] Essentially, the HBC is a "software agent that can be deployed on government OFFICIAL[133] IT devices, such as laptops, desktops, and servers [... to] collect[...] and analyse[...] technical metadata."[134] On that basis, the NCSC provides entities with "suspicious activity observations (SAOs)" and threat surface reports, which provide entities with indications for further analysis and can inform decisions on which log sources to monitor.[135] Thereby, HBC supplements the detection efforts of these entities. HBC's coverage comprises at least "370,000 Central Government endpoints"[136] (as of 2021) "across [a minimum of] 24 UK government organisations"[137] (2020).

Germany: Federal Security Operations Centre (BSOC) – Layer 1

The German Federal Office for Information Security (BSI) operates the Federal Security Operations Centre (Bundes Security Operations Centre, BSOC) whose tasks "include services for the collection and analysis of log and sensor data, as well as for the detection of and defence against malware in e-mails and web traffic."[138] These services are available for entities of Germany's federal administration. For example, the BSI—together with ITZBund, the German Federal Government's central IT service provider—offers "detection-as-a-service" (DaaS), through which entities may send their logging data to the BSI for analysis.[139] However, a July 2025 report by the German Bundesrechnungshof, Germany's federal court of auditors, reveals significant challenges in providing this service in practice. Of roughly 200 German public sector entities that could use the service, only five do so, with the BSI noting that both it and the potentially benefiting authorities lack the necessary personnel resources to expand DaaS quickly.[140] The BSOC also maintains cooperations with the authorities responsible for detection in

132 UK National Cyber Security Centre (2020): Host Based Capability. However, "any implementation costs (e.g. change request fees) will need to be covered by the recipient organisation."

133 OFFICIAL represents the lowest classification tier in the United Kingdom, UK Cabinet Office (2024): Government Security Classifications Policy.

134 UK National Cyber Security Centre (2021): Active Cyber Defence: The Fourth Year.

135 UK National Cyber Security Centre (2023): Active Cyber Defence: The Sixth Year.

136 UK National Cyber Security Centre (2022): Active Cyber Defence: The Fifth Year.

137 UK National Cyber Security Centre (2021): Active Cyber Defence: The Fourth Year.

138 Federal Office for Information Security (n.d.): Directorate-General OC -- Operative Cyber Security and Bundesamt für Sicherheit in der Informationstechnik (n.d.): Digitalisierung in der Bundesverwaltung absichern.

139 Bundesamt für Sicherheit in der Informationstechnik (2019): Engere Kooperation von BSI und ITZBund.

140 Bundesrechnungshof (2025): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit. In response, the German Federal Ministry of the Interior (BMI) and the Federal Ministry for Digital Transformation and Government Modernisation (BMDS) stated that they intend to expand DaaS and integrate it as a standard measure in federal IT consolidation. In its subsequent reaction to this statement, the Bundesrechnungshof criticized both ministries for leaving unclear how they plan to provide the BSI with the necessary resources in terms of personnel to implement the envisioned expansion (see further page 34 of the Bundesrechnungshof report).

Germany's 16 federal states.[141]

Given their importance to national cybersecurity, many NCAs also offer services to critical infrastructure or other domestic entities of essential importance within their jurisdiction. Providing support to them will often fall within an NCA's mandate to protect the nation against sophisticated cyber threats.[142] Depending on the institutional set up of a CI in a given country, these operators may be public (Layer 1) or private entities (Layer 2).

The services offered by an NCA to essential entities are typically offered free of charge on a voluntary basis or upon request. The scope and extent of these responsibilities usually depend on the type of actor and its criticality to functions of essential importance for the state. The support provided by an NCA is particularly important, as detection-related services are resource-intensive and therefore often limited in availability, which can lead to gaps in entities' detection posture.

Assistance by NCAs may include operating sensor networks to detect breaches across critical infrastructure sectors, actively searching for anomalies within networks and notifying entities when issues are identified, or helping them establish real-time monitoring capabilities. Oftentimes, the degree of NCA support possible will depend on the level of visibility granted by each entity into its operational environment.

Within the EU, the NIS 2 Directive provides for a national CSIRT's ability to "carry out proactive non-intrusive scanning of publicly accessible network and information systems of essential and important entities [...] to detect vulnerable or insecurely configured network and information systems and inform the entities concerned" (Art. 11(3)), thereby adding the carrying out of port scans[143] to the portfolio of CSIRT tasks.

Three examples of tasks undertaken by existing NCAs are presented in the following:

141 Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021.

142 For example, in listing the tasks of national CSIRTs, the EU's NIS 2 Directive also enumerates, upon request and vis-à-vis essential and important entities, the provision of "assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems" (Art. 11(3), point (a)), as well as, also upon request, the provision of a "proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact" (Art. 11(3), point (e)). The Directive specifies that "Member States shall ensure that their CSIRTs jointly have the technical capabilities necessary to carry out the[se] tasks" (Art. 11(2)).

143 "Running a port scan on a network or server reveals which ports are open and listening (receiving information) as well as revealing the presence of security devices, such as firewalls, that are present between the sender and the target," Palo Alto Networks (n.d.): What is a Port Scan?.

United States: CyberSentry Program – Layers 1 and 2 (depending on public/private set-up of CI)

CISA implements the so-called "CyberSentry Program," "a CISA-managed threat detection and monitoring capability that provides operational visibility into information technology and operational (IT/OT) networks within participating critical infrastructure entities," including via "unsupervised machine learning algorithms."[144] In practice, CISA informs entities when they identify any anomalous behavior in their networks and system and can subsequently support their remediation. For example, the program offered such assistance following the Solar Winds supply chain compromise.[145] Participation in the CyberSentry is voluntary and complimentary for U.S. critical infrastructure entities providing national critical functions for the United States, but requires the critical infrastructure entity to "provide access to in-depth network traffic and other telemetry."[146]

Norway: Operation of a national sensor network – Layers 1 and 2 (depending on public/private set-up of CI)

The Norwegian CERT (NorCERT) "operate[s] and organise[s] a national sensor network on the internet to detect data breaches in critical infrastructure across sectors."[147] Based on publicly available information, it remains unclear whether the network includes only sensors in critical infrastructure operated by the public sector or whether it also extends to private entities.

Germany: Searching for anomalies in critical infrastructure – Layers 1 and 2 (depending on public/private set-up of CI)

The German BSI—in addition to monitoring government networks—is also authorized to actively search for anomalies within critical infrastructure and is obliged to notify the respective operators if it detects suspicious behavior.

Activities in this area involve handling sensitive information, such as logs that could be relevant to states' intelligence efforts. As a result, NCAs directly supporting other states, for example in monitoring and analyzing their public sector networks (Layer 3) by sending personnel to another country to observe and detect malicious cyber activity, are less feasible at scale and require very close collaboration among the

144 U.S. Cybersecurity and Infrastructure Security Agency (2023): CyberSentry Program and Department of Homeland Security (2025): Cybersecurity and Infrastructure Security Agency – AI Use Cases. For further information on the use of machine learning algorithms within the CyberSentry program, see Critical Infrastructure Network Anomaly Detection (DHS-106) on the DHS website.

145 U.S. Cybersecurity and Infrastructure Security Agency (2023): CyberSentry Program.

146 U.S. Cybersecurity and Infrastructure Security Agency (2023): CyberSentry Program.

147 Norwegian National Security Authority (n.d.): Norwegian National Cyber Security Centre (NCSC) and NorCERT.

countries involved. Nonetheless, there have been efforts that fall under this category, notably the "hunt forward" operations (HFOs) conducted by the United States (for more information, see Chapter 7). Despite these rare cases, an NCA's collaboration with other states is generally more viable at a higher level, focusing on sharing information and guidance that support detection rather than direct involvement in detection-related monitoring and analytical tasks, as the next activity area will address.

Information Sharing and Operational Advice

NCAs play an important role as reliable information providers and advisors by outlining, for example, currently observed malicious behavior or emerging trends and providing detection-related guidance. Like the first activity area, the main target audience of the activity area information sharing and operational advice is domestic stakeholders (Layer 1 and 2), but the reach of these activities may also extend to international actors (Layer 3), especially when information and advice are provided publicly.

The role of an NCA as an information steward and advisor in a detection context may include the following activities, which are further elaborated below:

1. Sharing IoCs, TTPs, detection methods, vulnerability data and contextual intelligence (Section 6.2.1);
2. Facilitating (in)formal information-sharing arrangements and maintaining information services (Section 6.2.2);
3. Participating in (in)formal information-sharing arrangements (Section 6.2.3); and
4. Issuing recommendations, guidelines, and standards (Section 6.2.4).

Sharing IoCs, TTPs, detection methods, vulnerability data and contextual intelligence

The most publicly recognized activity that an NCA may undertake as an information provider is the issuance of alerts, advisories, and reports, which often share **IoCs** and **TTPs**.[148] This and other information shared by an NCA is essential, as it can contribute to reducing the time needed to detect specific threats, especially for organizations without in-house threat research teams. This information can be incorporated by the recipients into their own analytical efforts, for example, enabling them to compare it against collected logs to identify potential threats.

148 For example, U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

NCAs can and have in the past also used alerts, advisories, and other formats such as GitHub repositories to provide or verify specific **detection rules**. By turning threat intelligence into something actionable, NCAs can thereby provide operational advice for pathways for detecting specific malicious activities.

A few selected examples, among many more in practice, include the following:

United States, Poland, and United Kingdom: Joint Cybersecurity Advisory – Layers 1, 2, and 3

In December 2023, authorities from the U.S., Poland, and the United Kingdom issued a joint cybersecurity advisory on specific threat activity attributed to the Russian Foreign Intelligence Service. This advisory also contains advice on detection methods. Specifically, the advisory provides "SIGMA rules [that] target identified operators' behavior patterns [which] can be used for the threat hunting against collected logs," as well as YARA rules for "detect[ing] most known GraphicalProton variants."[149]

United States/United Kingdom: Advisories and Reports – Layers 1, 2, and 3

The U.S. CISA frequently publishes advisories and reports that also include downloadable SIGMA rules associated with the highlighted malware,[150] YARA rules,[151] and Snort signatures[152] for detection. The UK NCSC also issues malware analysis reports on a regular basis, which include similar information.[153] As part of its publicized advisories, CISA has sometimes also verified Suricata signatures provided by others by confirming their ability to detect exploitation attempts[154] or has pointed to other open-source detection rules made available, for instance, by industry.[155]

Belgium: Warning on Log4j vulnerability – Layers 1, 2, and 3

In its warning on the Log4j vulnerability, the Belgian Centre for Cybersecurity provided advice on detecting compromises by referencing external methods for network- and host-based detection, as well as open-source Snort and Suricata

---

149 U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): Joint Cybersecurity Advisory: Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally.

150 For example, U.S. Cybersecurity and Infrastructure Security Agency (2025): CISA Releases Malware Analysis Report Associated with Microsoft SharePoint Vulnerabilities.

151 For example, U.S. Cybersecurity and Infrastructure Security Agency (2025): MAR-251132.c1.v1 Exploitation of SharePoint Vulnerabilities.

152 For example, U.S. Cybersecurity and Infrastructure Security Agency and Multi-State Information Sharing and Analysis Center (2025): Joint Cybersecurity Advisory: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388.

153 UK National Cyber Security Centre (n.d.): Malware analysis reports.

154 For example, U.S. Cybersecurity and Infrastructure Security Agency and Multi-State Information Sharing and Analysis Center (2025): Joint Cybersecurity Advisory: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388.

155 For example, U.S. Cybersecurity and Infrastructure Security Agency, other U.S. agencies and international counterparts (2024): Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways.

rules.[156]

Japan: GitHub repository of YARA rules – Layers 1, 2, and 3

The Japanese Computer Emergency Response Team Coordination Center (JPCERT/CC) maintains a GitHub repository of YARA rules. The repository currently covers eight specific threat actors, including APT10 and Lazarus.[157]

The issuance of alerts and advisories also offers considerable potential for international collaboration, as demonstrated by the growing number of jointly published alerts and advisories. This also extends to collaboration with private sector entities or references to industry detection advice.[158] In the past, alerts and advisories increasingly included official public political attributions of threat activities to a particular state or APT group, underscoring the political implications of their threat assessment.[159]

In addition to specifying IoCs, TTPs, and detection rules, NCAs also play a significant role when it comes to circulating **vulnerability data and contextual intelligence** among various stakeholder groups.[160]

Two examples from the United States are as follows:

United States: 'Vulnrichment' initiative & Catalogue of known exploited vulnerabilities – Layers 1, 2, and 3

In 2024, U.S. CISA launched its "vulnrichment" initiative, which enriches Common Vulnerabilities and Exposures (CVE) data "with actionable data points like [e]xploitability [...], [t]echnical [i]mpact [...] and automatability."[161] Such information can guide prioritization on the basis of a more comprehensive picture. In addition, CISA maintains a catalogue of known exploited vulnerabilities (KEVs) which entities can use as detection input.[162]

156 Centre for Cybersecurity Belgium (2021): Warning : Active exploitation of a 0-day RCE in Log4j.
157 JPCERTCC: JPCERT/CC public YARA rules repository, GitHub.
158 For example, U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection acknowledges the collaboration with various private sector enterprises whose information supported the specific advisory or UK National Cyber Security Centre (2021): Microsoft update on brute force and password spraying activity refers to industry blog posts for advice that can inform an entity's detection efforts.
159 Christina Rupp and Alexandra Paulus (2023): Official Public Political Attribution of Cyber Operations: State of Play and Policy Options, Stiftung Neue Verantwortung.
160 Sven Herpig (2024): Vulnerability Disclosure: Guiding Governments from Norm to Action: How to Implement Norm J of the United Nations Norms of Responsible State Behaviour in Cyberspace, interface.
161 U.S. Cybersecurity and Infrastructure Security Agency (2025): Unlocking Vulnrichment: Enriching CVE Data and U.S. Cybersecurity and Infrastructure Security Agency: CISA Vulnrichment, GitHub.
162 U.S. Cybersecurity and Infrastructure Security Agency (2025): Known Exploited Vulnerabilities Catalog.

When sharing IoCs, TTPs, detection methods, vulnerability data, or contextual intelligence, NCAs should always have their constituencies in mind and, if necessary, tailor information for actionability across differing technical maturity levels to make it easier to process.[163] In sharing such detection-related information and providing operational advice, NCAs should consider integrating widely recognized taxonomies and frameworks so that their substantive input is comprehensible and easily shareable across jurisdictions and entities.[164]

Facilitating (in)formal information-sharing arrangements and maintaining information services

Information shared by NCAs may be public or restricted. Often, specific arrangements, such as the Traffic Light Protocol (TLP), can be used to maintain designated confidentiality levels across stakeholder groups. In addition, the impact and effectiveness of information-sharing arrangements often hinges on the submission and provision of information in standardized formats to ensure interoperability (see also, for example, footnote 164).

Depending on the type of information shared and target group envisioned, recipients may range from other public sector bodies to NCAs or companies in other countries that may rely on the shared information. The NIS 2 Directive also mandates European national CSIRTs to "provid[e] early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time" (Art. 11(3), point (b)).[165]

Against this backdrop, NCAs can play a crucial role in facilitating[166] the exchange of relevant information between various entities, especially at the domestic level. This is important for advancing detection ecosystems, since sharing information and operational advice (e.g. IoCs and other data discussed earlier) often relies on these arrangements being in place. These arrangements not only define how information is and can be shared but oftentimes also address other issues, such as exempting the sharing entity from potential liability claims.[167] The information received can also

163 On this aspect, see also FIRST (n.d.): Community and Capacity Building Initiatives - Actioning Alerts and Advisories (A4) and Hanneke Duijnhoven, Bram Poppink, Tom van Schie and Don Stikvoort (2021): Getting started with a national CSIRT.

164 For example, MITRE (n.d.): MITRE ATT&CK, OASIS (n.d): Structured Threat Information Expression (STIX) or OASIS (n.d.): Trusted Automated Exchange of Intelligence Information (TAXII).

165 Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), 2022/2555.

166 The NIS 2 Directive also includes a provision that EU Member States "shall facilitate the establishment of cybersecurity information-sharing arrangements" (Art. 29(3)) that enable "entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves" (Art. 29(1)), specifically when such information can contribute to threat detection – among other objectives.

support other detection-related functions of the NCA by helping to assess whether observed malicious behavior affects government or critical infrastructure networks and inform the issuance of (public) alerts.[168]

Broadly, there are two types of information-sharing arrangements that an NCA can facilitate:

1. **Bidirectional or multidirectional information-sharing arrangements** where the NCA shares information and members can also share with selected stakeholders, and
2. **Unidirectional information-sharing arrangements**, where the value lies mainly in the NCA providing specific information to particular member entities.

These arrangements often function as closed, members-only networks focused on particular constituencies such as within a single country (Layers 1 and 2) or across multiple jurisdictions (Layer 3). From the perspective of the NCA, their maintenance often requires significant resources, as such arrangements call for structures that enable—and if necessary, oversee—information exchanges.

As a side effect, arrangements of the first kind can also contribute to strengthening community-building. Their function in establishing and maintaining trusted relationships is crucial, as only then are participants willing to share in-depth information. Without trusted relationships, there may be reluctance to do so, even when sharing would be technically possible. In this regard, an NCA should pay due regard to the size of the group included, as this has implications for the level of trust possible and realistic.[169]

For example, in support of **bi- and multidirectional threat information sharing**,[170] existing NCAs maintain the following networks and platforms with entities ranging from domestic public sector entities (Layer 1) to national CSIRTs of other countries (Layer 3):

The Netherlands: National Detection Network (NDN) – Layers 1 and 2

The Dutch NCSC has been coordinating the National Detection Network (NDN) for

---

167 On participant protections in the context of threat information-sharing, see, for example U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Automated Indicator Sharing (AIS) Participant Protections.

168 The positive impact that the ability to receive and process information can have on detecting and analyzing adverse events is exemplified by the Salt Typhoon campaign. In this respect, former CISA Director Jen Easterly highlighted that industry partners played a crucial role in its detection by sharing threat intelligence with CISA and law enforcement, which "gave CISA and other federal government partners visibility into the breadth of the campaign," ultimately enabling deeper investigations and access to the threat actor's infrastructure – after "CISA threat hunters had previously detected the same actors in US government networks," (Comment by Jen Easterly on a LinkedIn post by Jeff Greene, Jeff Greene (2025): LinkedIn Post).

169 Otmar Lendl (2023): A Network of SOCs?, CERT.at.

170 Another example is the UK NCSC's management of the CISP (Connect, Inform, Share, Protect) platform for UK cybersecurity professionals, to be decommissioned in November 2025, UK National Cyber Security Centre (2025): Connect Inform Share Protect and UK National Cyber Security Centre (n.d.): Cyber-Security Information Sharing Partnership - Terms and Conditions v5.0.

more than 10 years.[171] Within the NDN, both Dutch authorities—specifically the NCSC alongside the Dutch General Intelligence and Security Service (AIVD) and the Dutch Military Intelligence and Security Service (MIVD)—as well as NDN members can share information (anonymously).[172] The NDN is open to Dutch government organizations and private-sector actors of vital importance as a complimentary service. In addition to its information-sharing function, the NCSC also "organises gatherings where [participants] can get to know each other" in an effort to exchange best practices and identify opportunities for collective analysis.[173]

Spain: National Network of SOCs (Red Nacional de SOC, RNS) – Layers 1, 2, and 3 (focus on 1 and 2)

After a pilot was started in 2021, the Spanish national CSIRT, the CCN-CERT, created the Spanish National Network of SOCs (Red Nacional de SOC, RNS).[174] It is open to five types of members: (a) Spanish public administration entities; (b) entities "provid[ing] SOC services in other entities, whether public or private, protecting Spanish assets," so-called provider entities; (c) private sector entities "with their own SOC protecting their Spanish assets"; (d) so-called "source entities" that do not take the form of a SOC but would like to contribute CTI; and (e) "liaison entities" offering exchanges with various communities.[175] As of October 31, 2025, the network comprised 147 Spanish public sector entities, 113 provider organizations, 23 private sector actors, two liaison organizations, and one source organization.

The network is primarily aimed at IoC sharing but also provides for the exchange of other relevant information such as "generic detection rules and use cases."[176] Exclusively for the RNS's public sector members, the network also provides "access to a sharing forum where they will exchange recommendations regarding the management and direction of the SOC [... s]uch as contracting models, recommendations on suppliers, [and] definition[s] of indicators for measuring services."[177] The network incentivizes the sharing of information by private and provider entities by measuring the degree of their participation, with the possibility of assigning gold- and silver-level status. This status can be important for these entities, since bodies of the Spanish public administration should take it into consideration "when evaluating commercial proposals from providers competing for public contracts."[178]

---

171 Dutch National Cyber Security Centre (2023): Analytic techniques and cybersecurity.

172 Dutch National Cyber Security Centre (2018): Nationaal Detectie Netwerk infosheet.

173 Dutch National Cyber Security Centre (n.d.): Participate in the NDN.

174 Sindicatura de Comptes de la Comunitat Valenciana (2023): Informe sobre las Actuaciones Realizadas por los Ayuntamientos Beneficiarios de las Subvenciones Destinadas a la Transformación Digital y Modernización, en el Marco del Plan de Recuperación, Transformación y Resiliencia, y de Seguimiento de las Recomendaciones sobre los Controles Básicos de Ciberseguridad: Ayuntamiento de València.

175 CCN-CERT (n.d.): National Network of SOCs (RNS).

176 CCN-CERT (n.d.): National Network of SOCs (RNS).

177 CCN-CERT (n.d.): National Network of SOCs (RNS).

178 CCN-CERT (n.d.): National Network of SOCs (RNS).

Luxembourg: Open Source Threat Intelligence and Sharing Platform (MISP) – Layers 1, 2, and 3

Developers of the Computer Incident Response Center Luxembourg (CIRCL), "a government-driven initiative," acting as "CERT for the private sector, communes and non-governmental entities in Luxembourg,"[179] created and maintain the Open Source Threat Intelligence and Sharing Platform (MISP, originally an abbreviation for Malware Information Sharing Platform).[180] CIRCL itself runs different MISP communities, including one for national/governmental CSIRTs in the European Economic Area or another one for financial sector entities with international membership.[181] Membership in the MISP communities is complimentary. Both the CIRCL and MISP community members can share CTI within selected groups in a structured manner.[182]

Japan: TSUBAME – Layer 3

In 2007, the Japanese JPCERT/CC launched TSUBAME, which it operated until the project was "temporarily suspended" in September 2024.[183] TSUBAME "install[ed] monitoring sensors in the national CSIRTs of the Asia Pacific region" that "gather[ed] and visualiz[ed] malicious Internet activities detected by each sensor, sharing this information among all members."[184] The project also aimed to enhance cooperation between CSIRTs in the Asia-Pacific region under the framework of APCERT.

Australia: Pacific Cyber Security Operational Network (PaCSON) – Layer 3

In 2017, the Pacific Cyber Security Operational Network (PaCSON) was created as an initiative by the Australian Department of Foreign Affairs and Trade (DFAT) with the objective of enhancing regional collaboration. PaCSON "maintains [...] operational cyber security points of contact and empowers members to share cyber security threat information [and] provides opportunities for technical experts to share tools, techniques and ideas."[185] The Australian Cyber Security Centre (ACSC) serves as the network's secretariat.[186] Membership is open to government representatives from the Pacific region, such as national CSIRTs or other representatives designated by their governments for this purpose.[187]

179 Computer Incident Response Center Luxembourg (n.d.): Mission Statement.
180 MISP, GitHub.
181 MISP Project (n.d.): MISP Communities and MISP Feeds.
182 Computer Incident Response Center Luxembourg (n.d.): MISP - Open Source Threat Intelligence Platform.
183 JPCERT/CC (2024): TSUBAME Info.
184 Information Security Policy Council Japan (2013): International Strategy on Cybersecurity Cooperation - j-initiative for Cybersecurity -.
185 Pacific Cyber Security Operational Network (n.d.): About us.
186 Pacific Cyber Security Operational Network (n.d.): Secretariat.
187 Pacific Cyber Security Operational Network (n.d.): Membership.

As a method of enabling **unidirectional threat information sharing**, some NCAs also maintain dedicated information portals or services:

United States: Shared Cybersecurity Services – Layer 1

Operating on a subscription basis, CISA provides domestic public sector entities such as "federal civilian departments and agencies [...] with cost-free access to commercial [...] CTI" in the framework of its Shared Cybersecurity Services (SCS).[188]

United Kingdom: Early Warning service – Layers 1 and 2

For "organisation[s] with a UK-based website," the UK NCSC provides an early warning service.[189] Building upon "information feeds from NCSC, trusted public, commercial and closed sources, which includes several privileged feeds [...] not available elsewhere," registered entities will receive—based on the information provided by them—customized daily and weekly information indicating incident notifications, network abuse events, and vulnerability and open port alerts.[190] To that end, "Early Warning does not conduct any active scanning of [the entities'] networks itself but uses information from other similar networks."[191]

Germany: Warning and Information Service (Warn- und Informationsdienst, WID) – Layers 1, 2, and 3

The German CERT-Bund, located within Germany's BSI, operates the Warning and Information Service (Warn- und Informationsdienst, WID). With Germany's federal administration as its primary audience, the WID provides all of its users—which may range from a CISO in a public sector entity (Layers 1 and 2) to an ordinary citizen (Layer 2, possibly also 3) with relevant information, such as alerts on exploited vulnerabilities or other "current threats to IT systems," aiming to deliver these in a timely manner.[192]

188 U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Cyber Threat Information Sharing (CTIS) - Shared Cybersecurity Services (SCS).
189 UK National Cyber Security Centre (n.d.): Early Warning.
190 UK National Cyber Security Centre (n.d.): Early Warning.
191 UK National Cyber Security Centre (n.d.): Early Warning.
192 Federal Office for Information Security (n.d.): Warning and Information Service (WID) and Bundesamt für Sicherheit in der Informationstechnik (n.d.): Warn- und Informationsdienst.

Participating in (in)formal information-sharing arrangements

In addition to facilitating information-sharing arrangements predominantly at the national level (Layers 1 and 2), NCAs often engage in cooperation at the international level (Layer 3). While such cooperation can take place on an ad hoc basis (e.g., when a country detects malicious activity in networks located within the jurisdiction of other countries or behavior suggesting that others may also have been affected), there are also more formalized and regular information-sharing arrangements at the 1) international, regional, and subregional levels or 2) bilateral levels. Examples of the former include participation in the following:

- 1a) **International networks** such as FIRST,[193] or
- 1b) **Regional platforms** such as the African Forum of Computer Emergency Response Teams (AfricaCERT), the Asia Pacific Computer Emergency Response Team (APCERT), the ASEAN Regional Computer Emergency Response Team, the CSIRTAmericas Network, the EU's CSIRTs Network, the Organisation of The Islamic Cooperation Computer Emergency Response Teams (OIC-CERT), the Pacific Cyber Security Operational Network (PaCSON), or TF-CSIRT.[194]

Examples of the latter include 2) **bilateral agreements** aimed at leveraging synergies in detecting malicious activities through enhanced information sharing, such as the UK–Republic of Korea Strategic Cyber Partnership[195] or the Canada–Ukraine Agreement on Security Cooperation.[196] However, given the high thresholds for sharing sensitive threat intelligence, it should be noted that there is no public indication as to whether any concrete steps were taken to advance these commitments in practice beyond mere political declarations of intent.

193 For instance, through the FIRST MISP information-sharing instance, FIRST (n.d.): FIRST Malware Information Sharing Platform (MISP) instance.

194 AfricaCERT (n.d.): About Us, APCERT (n.d.): About APCERT, Association of Southeast Asian Nations (2024): Secretary-General of ASEAN delivers remarks at the Opening Ceremony of the 9th ASEAN Ministerial Conference on Cybersecurity in Singapore, CSIRTAmericas Network (n.d.): Home, European Union Agency for Cybersecurity (n.d.): CSIRTs Network, Organisation of The Islamic Cooperation – Computer Emergency Response Teams (n.d.): OIC-CERT, Pacific Cyber Security Operational Network (n.d.): About us, and TF-CSIRT (n.d.): TF-CSIRT Community. For example, "in response to the Conti cyber threat, CSIRTAmericas, a network developed and operated by the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the [Organization of American States] OAS, distributed over 5,000 IOCs to 36 CSIRTs across 21 OAS Member States […] enabl[ing] OAS Member States to detect similar threats," Argentina, Australia, Brazil, Canada, Chile, Colombia, Czech Republic, Dominican Republic, Fiji, Germany, Israel, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay (2024): Joint Working Paper: How information sharing contributes to security and stability in cyberspace: Examples from Regional Points of contact networks.

195 The partnership identifies "detect[ing], disrupt[ing], and deter[ring] malicious cyber threats" as one of its core areas of cooperation and commits, inter alia, to "closely share information" and "establish a joint analysis group" in this regard, UK Foreign, Commonwealth & Development Office and Prime Minister's Office (2023): Republic of Korea-UK strategic cyber partnership.

196 The agreement stipulates: "The Participants will work together to enable Ukraine to detect, deter and disrupt Russian cyber aggression, cyber espionage and hybrid warfare, including through continuing cyber resilience and critical infrastructure protection, from malicious cyber activity [… inter alia] through cyber threat intelligence sharing," Global Affairs Canada (2024): Agreement on security cooperation between Canada and Ukraine.

Issuing recommendations, guidelines, and standards

NCAs are also exceptionally well-positioned to take on an advisory role that can support entities in establishing, enhancing, and standardizing their detection capabilities, for example, by sharing knowledge and identifying key areas to prioritize. Closely related, such efforts may also clarify specific requirements that certain entities may be obliged to follow by providing comprehensive frameworks to facilitate compliance. Such documents can, for example, provide recommendations on implementing specific tools to detect cybersecurity threats, offer guidance on prioritization in resource-limited environments, or define specific baseline requirements.

In addition to the possibility of providing dedicated guidance documents, NCAs can and have incorporated detection-related recommendations into their alerts and advisories.[197] Such inclusion can maximize the utility of advisories and contribute to their sustained relevance. Similar to alerts and advisories, issuing recommendations, guidelines, and standards offers great potential for international collaboration among NCAs. In doing so, NCAs can leverage synergies and expand the expertise available and their insights into relevant best practices.

Examples illustrating how NCAs have performed these functions—unilaterally or through international collaboration—include the following:

Australia, Canada, Czechia, Japan, New Zealand, Singapore, South Korea, United Kingdom, United States: Guidance on SIEM (and SOAR) implementation – Layers 1, 2, and 3

In May 2025, authorities from the Five Eyes countries alongside Czechia, Japan, Singapore, and South Korea jointly published three guidance documents offering advice on the implementation of SIEM and SOAR systems, as well as recommendations on which logs to prioritize when deciding what data to feed into a SIEM. The U.S. National Security Agency notes their particular relevance "for National Security Systems (NSS), the Department of Defense (DoD), and the Defense Industrial Base (DIB)."[198] These guidance documents also represent good communication practice, as they are tailored to different audiences and use wording adapted to each, thereby enhancing comprehensibility for various target groups.

---

197 For example, U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection provides recommendations for logging that can support "detect[ing] the activity described in this [cybersecurity advisory] CSA." See also Cyber Security Agency of Singapore (2025): Remediation Guide for a Compromised SharePoint Environment related to CVE-2025-53770 and CVE-2025-53771.

198 U.S. National Security Agency (2025): NSA, ASD's ACSC, and other agencies publish three Cybersecurity Information Sheets with guidance on SIEM and SOAR implementation.

Australia, Canada, the Netherlands, New Zealand, Singapore, South Korea, United Kingdom, United States: Joint baseline document outlining best practices for event logging and threat detection – Layers 1, 2, and 3

In August 2024, authorities from the Five Eyes,[199] Japan, the Netherlands, Singapore, and South Korea published a joint baseline document outlining best practices for event logging and threat detection, specifically targeting small and medium-sized businesses, large organizations, critical infrastructure, and government agencies alike.[200]

Germany: Orientation guide to using IDS & Minimum standard for logging and detecting malicious cyber activities – Layers 1, 2, and 3

In September 2022, Germany's national cybersecurity agency, the BSI, issued an orientation guide to using IDS.[201] The document "is intended as a guide to IDSs for operators of critical infrastructure and auditing bodies, as well as to the requirements that must be met when implementing such [a] system."[202] Earlier, in October 2018, the BSI published a minimum standard for logging and detecting malicious cyber activities, which defines the baseline requirements for federal information security in these areas. Implementation of this standard is mandatory for all entities within Germany's federal administration (Bundesverwaltung), and the BSI has continuously updated the standard since its introduction (most recently in November 2024).[203]

Operational, Financial, and Nonmaterial Assistance

NCAs also play an important role in providing operational, financial, and nonmaterial assistance, particularly among domestic nonpublic sector actors (Layer 2). This may include the following activities, which are further elaborated below:

- Developing and maintaining open source tools (Section 6.3.1);
- Providing funding (Section 6.3.2); and
- Collaborating with non-governmental stakeholders on research (Section 6.3.3).

199 Another relevant example from the Five Eye countries from September 2024 (updated in January 2025) is Australian Cyber Security Centre and international counterparts (2024): Detecting and mitigating Active Directory compromises.

200 Australian Cyber Security Centre and international counterparts (2024): Best practices for event logging and threat detection.

201 Bundesamt für Sicherheit in der Informationstechnik (2022): Orientation Guide to Using Intrusion Detection Systems (IDS).

202 Background for the issuance of the guide was that "operators of critical infrastructure and of energy supply networks are obliged to take steps to detect attacks as a way of protecting their information system" with IDS "form[ing] part of the compliance documents [to be] submitted" by them to the BSI, Bundesamt für Sicherheit in der Informationstechnik (2022): Orientation Guide to Using Intrusion Detection Systems (IDS).

203 Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen.

Developing and maintaining open-source tools

NCAs can leverage their expertise by developing and maintaining open-source tools that can serve as force multipliers by facilitating adoption in resource-limited contexts and reducing cost barriers.[204] These tools can be freely downloaded and used by entities to support their detection efforts, thereby contributing to the overall cybersecurity posture both domestically (Layers 1 and 2) and internationally (Layer 3). The functions are tool-specific but can, for example, facilitate log management and malware analysis.

Three examples of countries providing detection-relevant tooling are as follows:

United States: Logging Made Easy & Malcolm – Layers 1, 2, and 3

Since 2023, CISA has provided and maintained the "Logging Made Easy" (LME) tool (LME 2.0 since November 2024) on an open-source basis.[205] The tool offers a centralized log management solution with automatic alert components, enhancing entities' visibility and enabling any potential further analysis. LME can be downloaded by any entity but is particularly aimed at small and medium-sized organizations, particularly those without SIEM. These entities can download LME for free and run it locally within their IT perimeter.[206] Other examples are the open-source network traffic analysis tool Malcolm,[207] also (co)developed by CISA (first launched in 2019).

Canada: Assemblyline – Layers 1, 2, and 3

The Canadian Centre for Cybersecurity developed the malware detection and analysis tool Assemblyline, first launched in 2017, which "automate[s] the analysis of files [...] to better use the time of security analysts.[208]

Japan: LogonTracer and YAMA – Layers 1, 2, and 3

JPCERT/CC maintains the tools LogonTracer and Yet Another Memory Analyzer for malware detection (YAMA). LogonTracer, first launched in 2017, enables entities to

---

204 For an example at EU-level, see CERT-EU (2024): Sigma Unleashed: A Realistic Implementation.

205 The LME software stack combines three distinct open source software solutions: "Elastic Stack (for log management, search, and visualization), Wazuh (for endpoint detection and response), and Podman (for containerization)," U.S. Cybersecurity and Infrastructure Security Agency (2024): Logging Made Easy: Frequently Asked Questions.

206 U.S. Cybersecurity and Infrastructure Security Agency: LME, GitHub and U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Logging Made Easy.

207 For further information, see U.S. Cybersecurity and Infrastructure Security Agency: Malcolm, GitHub, U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Malcolm and Idaho National Laboratory (n.d.): Malcolm Tool Suite.

208 For further information, see Canadian Centre for Cyber Security: Assemblyline, GitHub and Canadian Centre for Cyber Security (n.d.): Assemblyline.

"investigate malicious logon by visualizing and analyzing Windows active directory event logs [... in an effort] to detect malicious hosts and accounts from event logs."[209] YAMA, first launched in 2023, seeks to address the challenge of "malware becom[ing] increasingly obfuscated and fileless" (which complicates detection) by enhancing a user's ability to conduct memory scans and thereby supporting the identification of malware of that type.[210]

Providing funding

The role of an NCA may also extend to providing financial support to certain entities, for example, to enable them to benefit from non-government-provided threat detection services. One example is past U.S. activity in this regard, with the caveat that the agreement providing U.S. funding for this program was terminated on September 30 this year:

United States: Multi-State Information Sharing and Analysis Center (MS-ISAC) – Layer 1

From 2005 until this year, the U.S. CISA—and previously the U.S. Department of Homeland Security—funded the Multi-State Information Sharing and Analysis Center (MS-ISAC), which offers various resources, including the sharing of threat intelligence and SOC services, to approximately 18,000 U.S. State, Local, Tribal, and Territorial (SLTT) government agencies.[211] The MS-ISAC was established in 2003 and is implemented by the Center for Internet Security (CIS, a U.S. non-governmental organization). The total government financial support received in 2024 was $27 million.[212] Since U.S. federal funding for MS-ISAC ceased, the CIS continues to operate the MS-ISAC on a "fee-based membership-model."[213]

Collaborating with non-governmental stakeholders on research

In addition to operational and financial support, NCAs may also support research efforts by providing non-material input and offering means to validate findings or

209 JPCERTCC: LogonTracer, GitHub.

210 JPCERTCC: YAMA, GitHub and JPCERT Coordination Center (2023): JPCERT/CC Activities Overview Topics: July 1, 2023 - September 30, 2023.

211 Center for Internet Security (n.d.): MS-ISAC: Defending America's Critical Infrastructure and Center for Internet Security (n.d.): MS-ISAC Services.

212 Zack Quaintance (31.07.2025): States Take Lead in Cyber Defense as Federal Support Shrinks, Industry Insider.

213 U.S. Cybersecurity and Infrastructure Security Agency (2025): CISA is Strengthening Our Nation's Security with Direct Cyber Support to State and Local Governments and Colin Wood (29.09.2025): CISA confirms it's ending MS-ISAC support, Statescoop.

collaborating on specific projects—activities that can not only advance external research but also allow an NCA to benefit from and possibly leverage their external expertise. As a positive side effect, such measures not only provide interesting research avenues (which ideally creates a win-win situation for both sides) but can also promote and positively contribute to a country's talent pipeline.

Two examples of tasks undertaken by existing NCAs include the following:

Germany: Provision of data and enablement of research opportunities – Layer 2

A German government agency, most likely the German BSI (although not explicitly stated), supports a Fraunhofer Institute by providing "real-world data" to help test and improve the researchers' open-source tool AMIDES. This tool uses machine learning to counter detection rule evasion.[214] The German BSI also encourages research on detection by inviting students to join the BSI as interns or to write their bachelor's or master's theses at the BSI, with a focus on designing, implementing, and testing methods for detecting malicious activities.[215]

Cyprus: Joint development and deployment of detection sensors – Layer 2

The Cypriot national CSIRT has worked with academia to develop and deploy detection sensors on critical government networks, helping to close capability gaps.[216] From the information publicly available, it is unclear what kind of data these sensors gather.

Examples

International detection capability-building, as discussed in this paper, is not a new concept. Some states, international organizations, and international and regional development banks are already engaged in international assistance projects—often under the label of CCB activities—aimed at enhancing cyber detection capabilities in other countries, which is a good sign. Yet, many of the relevant efforts currently underway tend to go largely unrecognized in terms of their policy importance and appear as isolated individual activities that are not put into a broader context with each other, limiting their strategic potential and the ability to amplify their impact.

The identified, already implemented international detection capability-building

214 Fraunhofer Institute for Communication, Information Processing and Ergonomics (2024): AMIDES Detects New Varieties of Cyberattacks.

215 Bundesamt für Sicherheit in der Informationstechnik (n.d.): Detektion von Angriffen auf Regierungsnetze.

216 Global Cyber Security Capacity Centre (2021): Cybersecurity Capacity Review: Republic of Cyprus.

actions cover a very broad spectrum. They encompass activities aimed at developing or enhancing some of the technology, people, and process capabilities discussed in the previous two chapters. Specifically, they range from support for the establishment of national CSIRTs—provided these also include any detection-related activities pertinent to monitoring, analysis, or information-sharing—or SOCs to the provision of training and workshops, as well as the hiring and financing of seconded personnel. Their scope varies depending on the financial and human resources invested, the actors funding and implementing them, and their time horizon. Mostly, donor governments invest in detection capability-building in certain priority regions, mostly in partner countries in or near their immediate geographical vicinity.

A few concrete examples from various regions show how certain countries and other funders are engaging in such activities (see Annex III for further examples):

- **United States → Costa Rica**: In March 2023, the United States pledged to spend $25 million dollars to "enable Costa Rica to *establish a national security operations center* [within the Costa Rican Ministry of Science, Innovation, Technology, and Telecommunications] to quickly detect and respond to cyber attacks and implement cybersecurity protections for its government systems."[217] This move came shortly after Costa Rica declared a state of emergency in 2022, following heavy targeting of government entities. In addition, the United States provided $10 million to build an entity-specific SOC within the Costa Rican Ministry of Public Security by the next year, with the assistance aimed at providing "state-of-the-art equipment, specialized training, and logistical support."[218]
- **European Union → Albania, Montenegro, and North Macedonia**: Through funding the Cybersecurity Rapid Response 2.0 project, which ran from April 2024 to September 2025 and was implemented by the Estonian e-Governance Academy (eGA), the EU aimed to "*increase [the] operational cyber capacities of Security Operations Centres* and Computer Security Incident Response Teams of beneficiaries" and to "improve inter-institutional information sharing"[219] as two of its primary objectives. The project has €4.4 million[220] in funding and its beneficiaries are Albania, Montenegro, and North Macedonia. One of the project outcomes is the opening of Montenegro's government SOC, during whose establishment phase eGA "supported [with] the procurement of necessary equipment."[221]
- **Germany → African Union Commission:** In 2024, Germany's development agency GIZ *hired an IT project officer* employed by the GIZ Addis Ababa field office and seconded to the African Union Commission (AUC)'s Management of Information Systems Directorate (MISD). The officer is *tasked with creating a SOC within the AUC*. His responsibilities include ensuring that the created SOC can, inter alia, "detect and take quick actions for any threats in the infrastructure of [the] AU" and "provide a

217 White House (2023): Statement by NSC Spokesperson Adrienne Watson on U.S. Cybersecurity Support to Costa Rica, Center for Strategic & International Studies (2023): A Conversation with Costa Rican President Rodrigo Chaves and U.S. Embassy in Costa Rica (2023): United States Announces $25 Million to Strengthen Costa Rica's Cybersecurity.

218 U.S. Embassy in Costa Rica (2023): United States Helps Strengthen Costa Rica's Cybersecurity and U.S. Southern Command (2023): Partnership with Costa Rica to Establish Cyber Security.

219 e-Governance Academy (n.d.): Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia 2.0.

220 e-Governance Academy (2024): High-level Opening of Montenegro Government Cybersecurity Operations Centre.

221 e-Governance Academy (2024): High-level Opening of Montenegro Government Cybersecurity Operations Centre. See also e-Governance Academy (2025): Strengthening cyber resilience with Security Operations Centres.

preventive monitoring of the IT infrastructure of the organization."[222]

- **Japan → Asia-Pacific region:** Detection capabilities played a role in various training programs carried out by Japanese entities, three of which are discussed. In October 2016, JPCERT/CC provided *log analysis training* for participants from Indonesia, Brunei, Cambodia, Laos, Myanmar, Timor-Leste and Vietnam in the framework of a project by the Japanese International Cooperation Agency (JICA).[223] As part of training for national CSIRTs, JPCERT/CC also *introduced its TSUBAME detection platform and assisted in the installation of sensors*, for example, in Vietnam.[224] In February 2020, JICA conducted a *cybersecurity seminar* in Myanmar for staff from Myanmar's National Cyber Security Center (NCSC), covering topics such as *network security and the role of government SOCs*.[225]
- **World Bank Cybersecurity Multi-Donor Trust Fund → Multiple countries**: For example, in Bangladesh, a 2017–2020 World Bank project supported the *development of strategic cyber awareness across critical information infrastructures by deploying coordinated cyber visibility measures and installing cyber sensors*, inter alia, to enhance their detection capabilities.[226] Another detection-relevant grant amounting to $200,000 was given to Mongolia in 2023 so that the newly established Mongolian national CSIRT can finance "several *innovative trials on the use of AI*" relevant to the performance of its functions. These pertain specifically to "*advanced threat detection*, by analyzing vast amounts of data and detecting patterns that may indicate the presence of a cyber threat or attack" and "real-time, continuous monitoring of data sources to identify and alert security teams about any unusual behavior or potential threats with higher precision."[227]

In addition to these activities, other relevant projects have been supported by the International Telecommunication Union (ITU) and the Inter-American Development Bank (IADB) or were provided in the context of the Tallinn Mechanism.

Most of the activities outlined above pertain mostly to international assistance from a development aid perspective. However, relevant state practice highlights that there is also a cyber-defense angle[228] to international detection capability-building, demonstrated by the following two publicly known example activities:

- **European Union → Moldova and Georgia**: Under the European Peace Facility (EPF),[229] the EU funds two assistance measures aimed at the Republic of Moldova and Georgia.[230] Like the EU's Cybersecurity Rapid Response 2.0 project, these assistance

222 GIZ African Union (2023): Principal IT Project Officer - African Union Commission, LinkedIn.
223 JPCERT/CC (2016): APT workshop and Log analysis training in Jakarta.
224 JPCERT/CC (2021): CSIRT Training to VNCERT/CC with JICA and Japan International Cooperation Agency (2022): Project on Capacity Building for Cyber Security in Vietnam (Career Development Plan): Project Completion Report.
225 Link not available anymore, a screenshot can be requested from the author.
226 Cybil Portal (n.d.): Project: Supply, Installation and Commissioning of Cyber Sensors into the CII for cybersecurity in Bangladesh.
227 World Bank (2023): 2023 DDP Annual Review.
228 "Practis[ing] detecting and collecting data about potential attackers" also formed part of an exercise for Ukrainian cyber professionals implemented in December 2024 in the context of the Tallinn Mechanism, e-Governance Academy (2024): Over 240 cyber professionals of Ukraine enhanced cybersecurity skills at the largest cyber exercise.
229 For an explanation of the EPF, see Christina Rupp (2024): Cyber Defence, Navigating the EU Cybersecurity Policy Ecosystem.
230 For more information on the cyber-defence related EPF measures towards Georgia with a detection component as implemented by eGA, see e-Governance Academy (2023): Memorandum with the Cyber Security Bureau of the Ministry of Defence of Georgia, e-Governance Academy (2024): eGA conducts cybersecurity trainings in Georgia and e-Governance Academy (n.d.): European Peace Facility Assistance on cyber defence in Georgia.

measures are also implemented by the eGA. In the case of Moldova, the "cybersecurity support [provided] aims to *increase the ability of the Moldovan Armed Forces and the Ministry of Defence to detect intrusions* into the information systems and to counter cyber-attacks."[231] The assistance measure, amounting to €4 million from December 2022 to September 2025, seeks to support Moldova through the provision of equipment and the organization of practical hands-on exercises.[232]

- **United States (+ Canada) → Multiple countries**: The United States, once jointly together with the Canadian Armed Forces,[233] also takes steps of a more interventionist nature under the pretext of enhancing detection capabilities in other states within the framework of what it calls "*hunt forward operations*".[234] In the context of these operations, U.S. Cyber Command—specifically the Cyber National Mission Force (CNMF)—personnel "deploy[s] to partner nations to observe and *detect malicious cyber activity on host nation networks*"[235] at their invitation. The United States envisions these efforts, usually a few months long, to contribute to building capabilities and personal connections[236] in the "host nation." The United States also asserts that there is an immediate benefit for its own constituents, such as government entities and critical infrastructure operators, as well as international counterparts, since it pledges to share insights on adversary behavior identified through HFOs—if permitted by the respective country.[237] The acting commander of the U.S. Cyber Command testified that, as of May 2025, "CNMF personnel have deployed more than 85 times to over 30 countries in partner-enabled missions to hunt on host networks."[238] This includes missions in Albania,[239] Croatia,[240] Estonia,[241] Latvia,[242] Lithuania,[243] Montenegro,[244] Ukraine[245] and Zambia.[246]

In addition to these "funder-to-country activities," relevant detection-related support can be provided also indirectly to partner countries. For example, governments may fund activities carried out by non-governmental organizations—such as the

231 e-Governance Academy (2024): European Union contributes to modernising Moldova's Cyber Defence with New Equipment.

232 See also e-Governance Academy (2024): Podcast ﷺ & blog: Enhancing cybersecurity in Moldova is a matter of survival, e-Governance Academy (2023): eGA and CybExer conducted live fire cybersecurity exercise for the Moldova's Ministry of Defence and e-Governance Academy (n.d.): European Peace Facility Assistance on cyber defence in Moldova.

233 U.S. Sixteenth Air Force (Air Forces Cyber) (2023): "Shared threats, shared understanding": U.S., Canada and Latvia conclude defensive Hunt Operations.

234 Jeff Kosseff (2024): The International Legal Framework for Hunt Forward and the Case for Collective Countermeasures, in: C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (eds.): CyCon 2024: Over the Horizon: 16th International Conference on Cyber Conflict.

235 U.S. Cyber Command (2022): Cyber 101: Hunt Forward Operations.

236 U.S. European Command (2022): Partnership in Action: Croatian, US cyber defenders hunting for malicious actors.

237 See, for example, U.S. Embassy in Albania (2023): "Commited Partners in Cyberspace": U.S. concludes first defensive Hunt Operation in Albania and U.S. Cyber Command (2020): Hunt Forward Estonia: Estonia, US strengthen partnership in cyber domain with joint operation.

238 U.S. Cyber Command (2025): Posture Statement of Lieutenant General William J. Hartman, USA, Acting Commander, United States Cyber Command Before the 119th Congress House Armed Services Committee Subcommittee on Cyber, Information Technologies, and Innovation.

239 U.S. Embassy in Albania (2023): "Committed Partners in Cyberspace": U.S. concludes first defensive Hunt Operation in Albania.

240 U.S. European Command (2022): Partnership in Action: Croatian, US cyber defenders hunting for malicious actors and Adam Janofsky (18.08.2022): Cyber Command deployed 'hunt forward' defenders to Croatia to help secure systems, The Record.

241 U.S. Cyber Command (2020): Hunt Forward Estonia: Estonia, US strengthen partnership in cyber domain with joint operation.

242 U.S. Sixteenth Air Force (Air Forces Cyber) (2023): "Shared threats, shared understanding": U.S., Canada and Latvia conclude defensive Hunt Operations.

243 U.S. Cyber Command (2022): U.S. conducts first Hunt Forward Operation in Lithuania and U.S. Cyber Command (2023): "Building Resilience": U.S. returns from second defensive Hunt Operation in Lithuania.

244 U.S. Cyber Command (2019): US, Montenegro work together to defend against malicious cyber actors.

245 U.S. Department of Defense (2023): Remarks by Assistant Secretary of Defense for Space Policy John Plumb at Center for a New American Security 2023 DOD Cyber Strategy Event and U.S. Cyber National Mission Force (2022): Before the Invasion: Hunt Forward Operations in Ukraine.

246 U.S. Cyber Command (2024): CNMF deploys first defensive cyber team to Zambia.

Australian, Swiss, and UK governments (and others) supporting the capacity-building work of FIRST,[247] or the UK Foreign, Commonwealth and Development Office (FCDO) funding the Shadowserver Foundation's dashboard, which provides various types of daily updated high-level information.[248] Sources like these can be leveraged by multiple governments in carrying out their detection responsibilities.

Challenges

Research into relevant examples of international detection capability activities, some of which are enumerated in the previous chapter (see Annex III for a full overview), has highlighted a challenge that pertains specifically to building incident detection capabilities worldwide: states and other funders pursue different angles and interests, carry out initiatives at varying levels, target diverse audiences, and allocate differing financial resources. This underscores the **complexity—or the fragmentation**[249] **—of capability-building efforts** spanning across numerous actors.

Even for a very specific focus area such as detection capabilities, it is difficult to gain a comprehensive overview, distinguish projects, or assess what has specifically been implemented beyond what is described in public summaries. Evaluating the concrete impact of these efforts on enhancing the detection maturity of public sector entities or national cybersecurity authorities is even more challenging.[250] This represents a challenge, as the difficulty in maintaining an overview can hamper coordination, which in turn may hinder the meaningful interplay of measures, especially since building detection capabilities is a long-term endeavor. Consequently, it may also lead to additional or overlapping activities that can further strain the already limited capacity of partner countries to absorb numerous capability-building offers.

In addition to these systemic challenges, two further categories of challenges may impede the development of capabilities necessary for carrying out governmental detection responsibilities. The first set involves **organizational, legal, and capacity-related constraints** that partner countries may face (Section 8.1). The second set concerns the **threat landscape and the adaptive TTPs of threat actors**, which make detection an increasingly complex endeavor and require entities to continuously refine their capabilities to account for these developments (Section

247 FIRST (n.d.): Community and Capacity Building Initiatives.

248 The Shadowserver Foundation (n.d.): Dashboard and The Shadowserver Foundation (n.d.): Dashboard overview.

249 Nayia Barmpaliou and Patryk Pawlak (2025): Between Ambition and Pragmatism: The future of cyber capacity-building in a fragmented world. According to Barmpaliou and Pawlak "operational fragmentation [is] driven by three key trends: the growth of the CCB community, the use of CCB by more communities of practice to pursue their objectives, and the widening gap between the aspirations for and realities of CCB coordination."

250 On evaluation challenges of CCB activities see also Phil Sheriff (2025): Does cybersecurity capacity building work?, Binding Hook.

8.2). Depending on their respective relevance to a specific partner country's context, these factors can influence the implementation of specific activities by shaping which capability-building measures are feasible despite particular challenges or by determining where targeted interventions could focus on addressing a challenge (or a set of related challenges) directly.

Organizational, Legal, and Capacity-Related Challenges

Some of the hurdles states face when seeking to build detection capabilities become apparent when examining Cybersecurity Capacity Maturity Model (CMM) reviews that employ the University of Oxford's Global Cyber Security Capacity Centre model.[251] Although some of these reports are becoming dated, they continue to offer a valuable baseline for assessing common detection challenges across national contexts.

The reports highlight various issues that have implications for a country's ability to comprehensively detect adverse behavior:

- Most evidently, the **absence of a national CSIRT**[252] **or government SOC**.[253] Such an institutional void can inhibit centralized coordination and visibility over national-level cyber threats, which in turn impairs detection response time and cross-sector information sharing;
- A **culture of concealing detected issues**, such as vulnerabilities, which persists because they are considered "confidential, commercially valuable information."[254] Concerns regarding data sensitivity and trust barriers can thus result in "no information [being] shared formally with other institutions, either within or across sectors,"[255] which impedes collective situational awareness and limits sector-wide learning from incidents. This lack of information sharing may be further reinforced by the absence or underenforcement of mandatory obligations to report detected issues and incidents at the national level;

251 Global Cyber Security Capacity Centre (n.d.): CMM Reviews Around the World. "The Cybersecurity Capacity Maturity Model for Nations (CMM) is a methodical framework designed to review a country's cybersecurity capacity. The CMM considers cybersecurity to comprise five Dimensions which, together, constitute the breadth of national capacity that a country requires to be effective in delivering cybersecurity: Developing cybersecurity policy and strategy; Encouraging responsible cybersecurity culture within society; Building cybersecurity knowledge and capabilities; Creating effective legal and regulatory frameworks; and Controlling risks through standards and technologies," Global Cyber Security Capacity Centre (n.d.): The CMM.

252 For example, Global Cyber Security Capacity Centre (2018): Cybersecurity Capacity Review: Bangladesh, Global Cyber Security Capacity Centre (2019): Cybersecurity Capacity Review: The Gambia and Cybersecurity Capacity Centre for Southern Africa (2023): Cybersecurity Capacity Review: Kingdom of Lesotho. ITU data from 2024 indicates that 28% of countries (55 out of 194) did not have a national CSIRT or were still in the process of setting one up (not yet accounting for differences in the maturity of existing CSIRTs), Robert Collett (2025): Cyber Capacity Building: A Primer for Diplomats, in: Andrea Salvi, Heli Tiirmaa-Klaar, James Andrew Lewis (eds.): A Handbook for the Practice of Cyber Diplomacy referencing International Telecommunication Union (2024): Global Cybersecurity Index 2024.

253 Global Cyber Security Capacity Centre (2021): Cybersecurity Capacity Review: Republic of Cyprus.

254 World Bank (2019): Cybersecurity Capacity Review: Cape Verde.

255 For example, Organization of American States (2020): Cybersecurity Capacity Review: Federative Republic of Brazil, World Bank (2019): Cybersecurity Capacity Review: Cape Verde, Global Cyber Security Capacity Centre (2019): Cybersecurity Capacity Review: The Gambia, World Bank and Global Cyber Security Capacity Centre (2017): Cybersecurity Capacity Review: Kyrgyz Republic, or ITU and Global Cyber Security Capacity Centre (2016): Cybersecurity Capacity Review of the Republic of Madagascar.

- **Limited detection capabilities among national critical infrastructures**, some of which are operated by domestic public sector entities such as small municipal governments, **leaving them very vulnerable to compromise.** Some CMM reviews note that detection capabilities across critical infrastructure are "uncoordinated and vary in quality," with various critical infrastructure operators lacking the required knowledge and expertise;[256] and
- **A country's private sector entities outpacing the public sector in detection capabilities**. For instance, in the case of Madagascar "only the major international institutions, primarily in the financial and telecommunications sector, along with some of the larger local companies, apply network intrusion detection systems or implement security operations centres."[257] Yet, it should be noted that this outpacing may apply to "only a very limited number of organisations"[258] in a country and that **capacities within the private sector can be distributed quite unevenly**. For example, a 2017 survey of 300 Swiss SMEs referenced in the country's CMM review came to the conclusion that "systems to detect cyber-incidents have been fully introduced in only a fifth of companies."[259]

Depending on local circumstances, challenges can also arise at a very practical level that may limit the availability of the infrastructure required for detection efforts. These include issues such as **infrastructure outages** or **unreliable internet connectivity**, which necessitate comprehensive backup solutions such as additional power generators.

With cybersecurity capability hinging on both resources and expertise, it is only consequential that CMM reports and other sources highlight additional fundamental challenges relating to **insufficient funding**, **shortages of skilled personnel, and brain drain**. In addition, in many states, salary competition from the private sector further exacerbates workforce retention challenges in public sector detection roles. In a detection context, the scarcity of personnel can become especially critical when large amounts of data are collected and aggregated, but few people are available—and have the necessary expertise—to analyze, make sense of, and act upon raw data such as atomic IoCs, which may contribute to "missing critical needles [—signals—] in the haystack."[260] Ukraine provides a telling example in this respect. In 2025, the country's Ministry of Digital Transformation highlighted that its "government institutions often face limited resources and a shortage of qualified specialists [that] prevents them from effectively monitoring threats in real time and responding quickly to cyber incidents."[261] Examples like these underscore the need

256 For example, World Bank and Global Cyber Security Capacity Centre (2018): Cybersecurity Capacity Review: Albania, Global Cyber Security Capacity Centre (2021): Cybersecurity Capacity Review: Republic of Cyprus, or Global Cyber Security Capacity Centre (2018): Cybersecurity Capacity Review: Independent State of Samoa.

257 ITU and Global Cyber Security Capacity Centre (2016): Cybersecurity Capacity Review of the Republic of Madagascar. See also World Bank (2019): Cybersecurity Capacity Review: Cape Verde and Global Cyber Security Capacity Centre (2021): Cybersecurity Capacity Review: Republic of Cyprus.

258 Global Cyber Security Capacity Centre (2018): Cybersecurity Capacity Review: Bangladesh.

259 Global Cyber Security Capacity Centre (2020): Cybersecurity Capacity Review: Switzerland.

260 Jayce Nichols (2025): Too many threats, too much data, say security and IT leaders. Here's how to fix that, Google Cloud.

261 Ministry of Digital Transformation of Ukraine (2025): Kitsoft Secures EU Grant to Build Cyber Defense Hub for Ukraine's Public Sector.

for strategic workforce development planning and investments in human resources—essentially the "people" component of a governmental detection capability.

Challenges Pertaining to the Threat Landscape and Threat Actor TTPs

From an entity perspective, the **complexity of ICT supply chains** makes effective threat detection more difficult. As organizations—and government entities alike—rely more heavily on wide networks of third-party providers and subcontractors, their attack surface expands beyond their direct control, which can obscure malicious cybersecurity events under the guise of legitimate activity.[262] This can complicate detection efforts, particularly where monitoring does not extend to third-party environments.

Additionally, specific (nation-state) threat actor behaviors pose challenges to building detection capabilities. For example, in July 2025, David Koh, the chief executive of Singapore's Cyber Security Agency, stressed that "between 2021 and 2024, [advanced persistent threat] APT activity detected in Singapore's cyberspace has more than quadrupled."[263] Hence, both the quantity and the increasing **sophistication of threat actor activities** require continuously adapting the necessary expertise and deploying advanced tools that can keep pace, which makes detecting such activities a highly complex and resource-intensive endeavor.

A few examples of relevant developments include the following:

- **Using "living off the land" (LOTL) techniques:** When publicly exposing the Volt Typhoon campaign and its prepositioning activities in U.S. critical infrastructure, authorities from the Five Eyes countries underscored that the Chinese state-sponsored threat actor behind it, like some of its counterparts in other states,[264] was actively employing measures to evade detection.[265] The advisory highlighted the deployment of LOTL techniques as one of the threat actor's TTPs. Specifically, LOTL techniques enable threat actors to "abuse [...] native tools and processes on systems [...] to blend in with normal system activities and operate discreetly with a lower likelihood of being detected or blocked because these tools are already deployed and trusted in the

262 For example, the French cybersecurity agency ANSSI has highlighted this risk, citing a case in which a foreign IT subcontractor – working with several major French companies – was compromised. This breach allowed the threat actor to infiltrate the companies' information systems through legitimate access channels and leveraging trusted infrastructure, French Cybersecurity Agency (2025): Cyber Threat Overview 2024.

263 Cyber Security Agency of Singapore (2025): Welcome Remarks by Mr David Koh, Chief Executive of CSA at the Operational Technology Cybersecurity Expert Panel Forum.

264 See, for example, U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): Joint Cybersecurity Advisory: Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally.

265 U.S. Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure and U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. See also Microsoft (2023): Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.

environment."[266] As a result, by seeking to achieve objectives via built-in infrastructure within a target entity, threat actors can help avoid alerts that would otherwise be triggered once third-party applications are installed.[267] Hence, LOTL complicates signature-based detection and requires the implementation of behavioral baselining and analytics to spot behavior employing these techniques.

- **Deleting event logs**: In addition to employing LOTL techniques to cover their tracks, many threat actors also try to eliminate any data that could reveal their presence or activity within an entity's operational environment, for example by deleting event logs and clearing other related information. The usage of such a technique was, for example, observed in Sandworm's NotPetya operation,[268] as well as activities by various threat actors including Volt Typhoon,[269] APT28, and APT38.[270]
- **Disabling detection systems**: Cyber agencies around the globe have also underscored that state-backed actors seek to delay the detection of their operations by disabling dedicated detection systems in targeted networks. In this respect, a BSI report notes the emergence and spread of so-called "EDR killers" and their availability as malware-as-a-service (MaaS).[271]
- **Employing means to act anonymously**: In addition, threat actors are actively using anonymization networks to evade and complicate their detection, including the use of botnets or "commercial VPNs, TOR, and proxy software."[272]
- **Cloud implications:** Threat researchers have further highlighted that threat actors are increasingly moving their operations to the cloud, offering them the potential of leaving no trace (e.g. on endpoints) which makes their activities even harder to detect, especially for entities with limited resources.[273]
- **Leveraging "AI-enabled automation to aid evasion and scalability":**[274] Threat actors are increasingly using automation, machine learning, and AI to create more contextualized and adaptive malicious activities.[275] This poses a significant challenge for entities attempting to detect such activities, as they differ from previously observed patterns in CTI and therefore cannot be easily incorporated into an entity's (automated) analytical systems. Hence, the UK NCSC assesses that such "human-machine teaming will highly likely make the identification, tracking and mitigation of threat activity more challenging without the development of effective AI assistance for defence."[276]

Even though the global median dwell time—the time "an attacker is on a system from compromise to detection"[277] —has decreased overall in recent years, all these

266 Australian Cyber Security Centre and international counterparts (2024): Identifying and Mitigating Living Off the Land Techniques.

267 U.S. Cybersecurity and Infrastructure Security Agency, other U.S. authorities and international counterparts (2023): People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.

268 Cisco Talos (2017): New Ransomware Variant "Nyetya" Compromises Systems Worldwide.

269 U.S. Cybersecurity and Infrastructure Security Agency, National Security Agency and Federal Bureau of Investigation (2024): PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

270 MITRE (2025): Indicator Removal: Clear Windows Event Logs.

271 Bundesamt für Sicherheit in der Informationstechnik (2024): Die Lage der IT-Sicherheit in Deutschland 2024. See also MITRE (2025): Impair Defenses: Disable or Modify Tools.

272 For example, European Union Agency for Cybersecurity (2024): ENISA Threat Landscape 2024 and French Cybersecurity Agency (2025): Cyber Threat Overview 2024. See also Michael Raggi (2024): IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders, Mandiant Google Cloud.

273 Florian Roth (2025): LinkedIn Post.

274 UK National Cyber Security Centre (2025): Impact of AI on cyber threat from now to 2027.

275 See, for example, Google Threat Intelligence Group (2025): Adversarial Misuse of Generative AI.

276 UK National Cyber Security Centre (2025): Impact of AI on cyber threat from now to 2027.

277 Google Cloud Security (2024): Special Report: Mandiant M-Trends 2024.

challenges can delay the mean time to detect (MTTD),[278] if a threat behavior is detected at all. Such delays can amplify the activity's spread, potential damage incurred, and possible data exfiltration.

Considerations for Designing International Detection Capability-Building Actions

This paper made the case for why policy-makers should increasingly leverage detection capability-building as a strategic opportunity. Especially from a cyber diplomacy standpoint, such efforts not only strengthen an essential cybersecurity capability in partner countries but also offer a significant pathway for accelerating the implementation of the framework of responsible state behavior. Nonetheless, while the link between capability building and norms implementation is, in theory, widely recognized and reflected in policy documents and UN discussions,[279] the connection remains largely indirect in practice.

Detection capabilities provide a prime example of why this is a missed opportunity: although they clearly enable states to implement the majority of these norms (see Chapter 3), activities aimed at their development rarely highlight their relevance to high-level UN policy discussions. Making such links more explicit could support raising awareness. This does not necessarily call for changing specific elements of capability-building actions. States can already invest in small steps, such as adjusting the framing and (political) embedding of a specific activity. This, in turn, could contribute to strengthening political buy-in, demonstrating the practical relevance of norms to technical communities, and fostering broader internal socialization of norms across government entities.

States seeking to support other countries in building or enhancing detection capabilities can use the activities outlined in Chapters 5 and 6 as a starting point. These activities provide examples of what could be done; they are not prescriptions for what should be done or what is right in a specific context. In other words, they can serve as inspiration for identifying needs and setting specific cyber-related development goals aligned with local realities and priorities. The specific interventions and measures chosen should always be tailored to a partner country's existing capacities and unique circumstances.

278 Splunk (2024): What Is MTTD? The Mean Time to Detect Metric, Explained.
279 For example, in 2022, EU Member States "emphasi[zed] the need to better connect the EU's cyber capacity building strategy with the UN norms of responsible State behaviour in cyberspace," Council of the European Union (2022): Council conclusions on the development of the European Union's cyber posture, 9364/22.

Importantly, care should be taken to ensure that the recipient country or organization has the capacity to absorb the proposed assistance. In many cases, there may be more offers of support than can be effectively accepted or implemented at one time. It is therefore essential to engage in consultation—at least with like-minded partners active in the relevant region or partner country—to avoid introducing additional activities that could further strain a partner country's or region's already limited capacity to absorb numerous capability-building offers. It is also important to re-emphasize that building detection capabilities requires strategic long-term patience and continuous investment in technology, people, and processes.

To support potential coordination among interested donor governments, Annex III provides a mapping of relevant publicly known activities. This overview can aid decision-makers in identifying already existing support, assessing potential overlaps with planned activities, and exploring opportunities to leverage synergies with others in the area of international incident detection capability-building.

In light of the challenges outlined in the previous chapter, policymakers should consider three overarching factors when planning actions to build detection capabilities in partner countries, using them to guide context-specific decisions:

Consideration 1: Basics first

Building detection capabilities should proceed in small, deliberate steps, beginning with policy, organizational, and governance prerequisites before moving to more advanced measures. Donor states considering international assistance should first assess whether these foundations are in place. In this respect, states should give due consideration to the measures stipulated in existing relevant frameworks and standards as baselines.[280]

Depending on local circumstances, foundational prerequisites can include a clear governance structure laying out roles and responsibilities, defining reporting lines, and ensuring relevant legal requirements (if any) are understood or developed wherever necessary. Taking steps toward establishing and maintaining reliable, up-to-date asset inventory of hardware and software used in specific infrastructures is also critical. Without a comprehensive overview of what is to be defended—and should form part of an entity's detection coverage—resources risk being wasted without effectively advancing an entity's detection posture. Complementary measures such as risk management profiling and employee awareness initiatives can

280 For example, National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0, International Organization for Standardization and International Electrotechnical Commission (2022): ISO/IEC 27001:2022 or International Organization for Standardization and International Electrotechnical Commission (2022): ISO/IEC 27002:2022.

further strengthen this foundation.

Once these fundamentals are in place, efforts can progress to more advanced technical measures. The next steps should begin with targeted initiatives, based on a logging policy that is already in place or to be developed, to build partner countries' capabilities to monitor and analyze selected government networks or critical infrastructure operators, with the option for gradually expanding coverage as capacity grows. While this paper focused specifically on detection capabilities, it is important to also pay attention to integrate detection in the rest of the defense process by ensuring, or working towards, a basic level of response capability before proceeding with technical detection measures. Otherwise, anomalous behavior would be ideally spotted and understood, but the entity would lack the basic means to act on detected incidents.

Consideration 2: Leverage unique added value

Policymakers should keep in mind that the end goal of a governmental detection capability is not necessarily for public-sector entities to carry out all responsibilities on their own. Instead, capability development efforts should focus on areas where public sector entities can provide the greatest added value in monitoring their own operational environments and fostering detection across a country's jurisdiction. When designing an intervention logic, decision-makers in donor and partner countries therefore need a clear understanding of where public-sector action can have the highest impact to fulfill governmental detection responsibilities.

Governments should avoid investing in measures that risk duplicating existing efforts or have poor long-term cost–benefit ratios, such as highly specialized and resource-intensive capabilities that can be accessed more efficiently by involving external expertise.[281] However, careful balancing is required; while leveraging the potential of outsourcing certain tasks, particularly as a transitional solution in lower–maturity contexts, it should remain the objective that the most critical functions are developed and maintained in–house to mitigate dependency risks.

Consideration 3: Invest in people and community building

The effectiveness of detection capabilities depends less on the technology itself and

281 It is also important to constantly evaluate the cost–impact ratio of specific measures – both when establishing new functions and reviewing existing ones – against the backdrop of other available (commercial) resources to ensure efficiency and effectiveness. A concrete example illustrating this need is the UK NCSC's Cyber Threat Intelligence Adaptor, "a software program [...] enabl[ing] authorised organisations to receive a high-quality, contextually-rich, cyber threat intelligence feed from the NCSC," which the NCSC retired in 2023. NCSC argued that it ended the program "considering the project outcomes against ongoing development of commercial products," UK National Cyber Security Centre (2023): Active Cyber Defence: The Sixth Year.

more on the people who are needed to turn information into actionable insights. Being able to do so depends heavily on sociotechnical and analytical skills, including understanding the technology and one's environment (e.g., typical user behaviors and log-in patterns) and building relationships across entities to exchange relevant information, best practices, and lessons learned. Donor countries must therefore take heed of the fact that it is essential to invest in developing a robust and diverse cybersecurity talent pipeline.[282] Efforts may also engage the existing limited workforce to reduce turnover or brain drain. Relevant activities could center on supporting domestic training and education programs at public sector institutions and key public universities.[283]

In addition, in resource-limited settings, strong communities can compensate more effectively for financial and personnel constraints than technology alone, but this requires opportunities to build mutual trust. When identifying potential areas of activity, decision-makers in donor countries should therefore also consider supporting nontechnical measures, such as efforts aimed at community building. This could be done by facilitating interactions between experts, for example, at the analyst-to-analyst level or participation in domestic or regional conferences. Given the limited duration of many foreign assistance projects, fostering trusted environments at the personal level through measures like these can enhance sustainability of projects, as outputs from these efforts can be leveraged and further developed even after their conclusion.

Annex

282 Sven Herpig (2025): Building a Sustainable Cybersecurity Talent Pipeline: Unlocking the Potential of the German–Philippine Defense Cooperation, Konrad Adenauer Foundation.

283 For example, to determine which skills to focus on, the following frameworks can serve as inspiration: U.S. Cybersecurity and Infrastructure Security Agency (2025): NICE Workforce Framework for Cybersecurity (NICE Framework) and European Union Agency for Cybersecurity (2022): European Cybersecurity Skills Framework Role Profiles.

Annex I: Selected Statements by UN Member States on Detection/Detection Capabilities in the Framework of the UN OEWG

Search...

Country	UN Regional Group	Month/Year	Agenda Item	Relevant Excerpt of Statement
Antigua and Barbuda	Latin America and Caribean States	December 2023	Capacity-building	"Chair, in response to your guiding questions, Antigua and Barbuda, as technical expertise, incident response capability to include simulated p towards response to attacks on critical infrastructures, and recognizing foundational capacities required for states to **detect**, defend against, or "We are of the firm view that starting with these critical baseline setting Barbuda will be much better able to protect our critical infrastructure ar institutional dialogue and transboundary **threat detection**."
Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Mexico, Paraguay, Peru, the Dominican Republic and Uruguay	Latin America and Caribean States	December 2023	Capacity-building	"We should also like to emphasize that the creation and maintenance o in each of the spheres of this Open-ended Working Group. For example **capacity to detect and deal with threats**. So therefore, building and mai environment that's safer for everybody."
Belgium	Western European and other States	March 2024	Existing and potential threats	"We stress it at each of our sessions, Mr. Chair, but this is the evolving year, cyber threats have further intensified and gained in complexity wi scale and innovative methods being employed to exploit vulnerabilities, Ransomware has grown in both scale and sophistication and the develo and generative AI systems have lowered the barriers of entry for cyber malicious activities – such as fraud, misinformation and deep fakes, enl **detection evasion**. This increasingly complex global threat landscape u concerted international efforts to enhance cybersecurity and safeguard fundamental character of the "threat" pil[l]ar of our Group's work." "The accessibility of generative AI lowers the entry barrier for cybercri sophisticated phishing campaigns and malware with ease. Even seasor integrating LLMs into their malicious pipelines. Researchers have demo malware to **evade detection**, generating malicious code on-the-fly usin malware solutions may struggle to **detect** this novel approach, requiring **techniques**. The cybersecurity landscape must adapt rapidly to this em solutions to protect against the misuse of LLMs."
Canada	Western European and other States	March 2024	Existing and potential threats	"Additionally, AI and more specifically machine learning-enabled techn manufacture and harder to **detect**, which compounds the number and s may face tomorrow."

‹ 1 / 13 ›

For a complete presentation of this graph, please see the online version of this publication.
https://www.interface-eu.org/publications/international-detection-capability-building

To see the table in a new tab, click here.

Annex II: How Detection Capabilities Are Reflected in Relevant UN Norms Guidance Documents

Search...

UN Cyber Norm	UN Cyber Norm - Full Text	UN GGE 2021 Norms Implementation Guidance	UN GGE 2021 Norms Implementation Guidance - F
Norm A: Interstate cooperation on cybersecurity	"Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security."	✗	
Norm B: Consider all relevant information	"In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences."	✗	
Norm C: Prevent misuse of ICTs in your territory	"States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."	✓	"This norm reflects an expectation that if a State is in good faith that an internationally wrongful act c emanating from or transiting through its territory it and reasonably available and feasible steps to **det** address the situation." "The norm raises the expectation that a State will within its capacity to end the ongoing activity in its means that are proportionate, appropriate and effe consistent with international and domestic law. No **expected that States could or should monitor all IC territory.**"

1 / 4

For a complete presentation of this graph, please see the online version of this publication.
https://www.interface-eu.org/publications/international-detection-capability-building

To see the table in a new tab, click here.

Annex III: Mapping of International Efforts to Build Detection Capabilities

Search...

Donor	Partner Country, Region or Organization	Year	Elements of Activities Aimed at Enhancing Detection Capabilities
European Union (Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia 1.0)	Albania, Montenegro, North Macedonia	2022-2024	Support the "improvement of **Computer Security Incident Response Teams'** organisational capacity"
European Union (Cybersecurity Rapid Response for Albania, Montenegro and North Macedonia 2.0)	Albania, Montenegro, North Macedonia	2024-2025	"Increase operational cyber capacities of **Security Operations Centres** and **Computer Secu Response Teams** of beneficiaries"
World Bank (Cyber Trust Fund)	Angola	2023	Support Angola in building its "technical and operational capabilities to **detect**, respond to, cyber incidents and protect critical information infrastructure" by "identifying the main gap devis[ing] a strategy and action plan to strengthen the overall cybersecurity maturity" (p. 1
Japan (Japan Computer Emergency Response Team Coordination Center, JPCERT/CC)	ASEAN countries (Indonesia, Brunei, Cambodia, Laos, Myanmar, Timor-Leste, Viet Nam)	2016	"APT (Advanced Persistent Threat) workshop and **log analysis** training" conducted from Oc 2016, in Indonesia, with hands-on training on "**detecting** traces of attacks" by "analyzing sa proxy servers and Active Directory based on an APT attack scenario"
ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBA)	ASEAN Member States	2022	Exercise for **Security Operation Center (SOC)** analysts where participants are "provided wit comprehensive knowledge and necessary skills" in the areas of cyberattack methods, "sec products to **detect** and prevent cyberattacks", and analysis of **detected** attacks to "become analyzing security incidents"

‹ 2 / 18 ›

For a complete presentation of this graph, please see the online version of this publication.
https://www.interface-eu.org/publications/international-detection-capability-building

To see the table in a new tab, click here.

Annex IV: Glossary

	Definition	Source
adverse event analysis	"Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents."	National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0
capability	"a measurable activity that may be performed as part of an organization's roles and responsibilities"	FIRST (2019): FIRST CSIRT Services Framework Version

		2.1
capacity	"the number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion"	FIRST (2019): FIRST CSIRT Services Framework Version 2.1
cloud security posture management	"the process of monitoring cloud-based systems and infrastructures for risks and misconfigurations"	Microsoft (n.d.): What is CSPM?
Computer Security Incident Response Team	"an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission"	FIRST (2019): FIRST CSIRT Services Framework Version 2.1
continuous monitoring	"Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events."	National Institute of Standards and Technology (2024): The NIST Cybersecurity Framework (CSF) 2.0
cyber capacity-building	"an umbrella concept for various types of activity in which individuals, organizations and governments collaborate nationally or across borders to develop capacity and capabilities that mitigate cyber risks to the safe, secure and open use of information and communications technologies (ICTs)"	Joyce Hakmeh, Amrit Swali and Robert Collett (2024): A principles-based approach to cyber capacity-building (CCB), Chatham House
cybersecurity event	"an occurrence of a system, service or network state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security"	Australian Cyber Security Centre (2025): Guidelines for cybersecurity incidents
cybersecurity incident	"an unwanted or unexpected cybersecurity event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations"	Australian Cyber Security Centre (2025): Guidelines for cybersecurity incidents
detection	"the monitoring and analyzing of system events to identify unauthorized attempts to access system resources"	Canadian Centre for Cyber Security (2020): Assemblyline
detection capabilities	hardware- and software-based technical tools (technology), human expertise (people), and procedural mechanisms (processes) to monitor and analyze cybersecurity events – "any observable occurrence[s] in a network or system" – in order to identify unauthorized access attempts within designated IT environments	Own definition
detection use case	"specific condition to be detected by a [CSIRT's] Information Security Event Management service	FIRST (2019): FIRST CSIRT

	area"	Services Framework Version 2.1
dwell time	the time "an attacker is on a system from compromise to detection"	Google Cloud Security (2024): Special Report: Mandiant M-Trends 2024
endpoint detection and response	"The term "endpoint detection and response" means cybersecurity tools and capabilities that combine real-time continuous monitoring and collection of endpoint data (for example, networked computing device such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities."	Executive Office of the President (2025): Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity
extended detection and response	"XDR is a software as a service tool that offers holistic, optimized security by integrating security products and data into simplified solutions. [...] In contrast to systems like endpoint detection and response (EDR), XDR broadens the scope of security, integrating protection across a wider range of products, including an organization's endpoints, servers, cloud applications, emails, and more. From there, XDR combines prevention, detection, investigation, and response to provide visibility, analytics, correlated incident alerts, and automated responses to improve data security and combat threats."	Microsoft (n.d.): What is a security operations center (SOC)?
"living off the land" techniques	"LOTL involves the abuse of native tools and processes on systems, especially living off the land binaries, often referred to as LOLBins, to blend in with normal system activities and operate discreetly with a lower likelihood of being detected or blocked because these tools are already deployed and trusted in the environment."	Australian Cyber Security Centre and international counterparts (2024): Identifying and Mitigating Living Off the Land Techniques
log	"a record of the events occurring within an organization's systems and network" "logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network"	National Institute of Standards and Technology (n.d.): Glossary - Log Executive Office of the President (2025): Executive Order 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity
log aggregation	"consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event"	National Institute of Standards and Technology (n.d.): Glossary - Aggregation
log analysis	"study[... of] log entries to identify events of	National Institute of

	interest or suppress log entries for insignificant events"	Standards and Technology (n.d.): Glossary - Log Analysis
log collection	the process of automatically transferring events to be logged to a central logging infrastructure and storing them there	Bundesamt für Sicherheit in der Informationstechnik (2024): Mindeststandard des BSI zur Protokollierung und Detektion von Cyberangriffen
log management	"process for generating, transmitting, storing, analyzing, and disposing of log data"	National Institute of Standards and Technology (n.d.): Glossary - Log Management
log management infrastructure	"the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data"	National Institute of Standards and Technology (n.d.): Glossary - Log Management Infrastructure
log retention	"archiving logs on a regular basis as part of standard operational activities"	National Institute of Standards and Technology (n.d.): Glossary - Log Retention
international detection capability-building	supporting partner countries or international organizations in strengthening their technology, people, and process capabilities to monitor events and identify adverse cyber events and incidents	Own definition
intrusion detection systems	"tool that detects security-relevant events on a system or network basis and helps to evaluate, escalate and document them. Security-relevant events can be detected based on patterns and/or anomalies"	Bundesamt für Sicherheit in der Informationstechnik (2022): Orientation Guide to Using Intrusion Detection Systems (IDS)
operational environment	all assets, systems, services, interfaces, and environments used for information processing, including on-premise systems, networks, and cloud-based infrastructure of an entity	Own definition
port scans	"running a port scan on a network or server reveals which ports are open and listening (receiving information) as well as revealing the presence of security devices, such as firewalls, that are present between the sender and the target"	Palo Alto Networks (n.d.): What is a Port Scan?
security information and event management system	"a type of software platform or appliance that collects, centralises, and analyses log data from sources within a network or system for the purpose of cyber security. If properly implemented for this purpose, a SIEM platform	Australian Cyber Security Centre and international counterparts (2025):

	automates the collection and centralisation of important log data that would otherwise be scattered across a network, thus making it easier for a human security team to navigate. Unlike some other log collection and centralisation tools, a well-configured SIEM then applies a predefined baseline of business-as-usual network activity, rules and filters to analyse and correlate the log data. This analysis can allow the SIEM platform to detect unusual activity on the network, which may represent a cyber security event or incident. Most SIEM products enhance their analysis by incorporating up-to-date threat intelligence."	Implementing SIEM and SOAR platforms: practitioner guidance.
security operations centre	"a centralised facility within an organisation, responsible for activities such as security monitoring and incident management"	UK National Cyber Security Centre (n.d.): Glossary
security orchestration, automation, and response	"a type of software platform that builds upon the collection, centralisation, and analysis of log data. Some SOAR platforms perform these functions themselves, while others integrate with an existing SIEM and leverage its log collection, centralisation, and analysis. Either way, a SOAR automates some of the response to detected cyber security events and incidents. It does so by applying predefined 'playbooks', which set certain actions to be taken when specific events occur, such as isolating the source of the event in the network. These automated actions do not replace human incident responders but can complement them."	Australian Cyber Security Centre and international counterparts (2025): Implementing SIEM and SOAR platforms: Executive guidance
SIGMA rules	"Sigma is a generic and open signature format that allows [someone] to describe relevant log events in a straightforward manner. The rule format is very flexible, easy to write and applicable to any type of log file."	SigmaHQ, GitHub
Snort signatures	"Snort rules consist of headers and options that define actions (e.g., alert, log, drop), protocols, IPs, and traffic patterns, enabling tailored protection against threats like malware, unauthorized access, and data exfiltration."	Splunk (2024): Snort Rules 101: Examples & Use Cases for Snort Network Defense
standard operating procedures	"formal, written guidelines or instructions for incident response that typically have both operational and technical components"	U.S. Cybersecurity and Infrastructure Security Agency (n.d.): Standard Operating Procedures (SOPs)
Suricata rules/ signatures	"Suricata is a high performance Network IDS, IPS and Network Security Monitoring engine. [...] A rule/signature consists of the following: The action, determining what happens when the rule matches. The header, defining the protocol, IP addresses, ports and direction of the rule. The rule options, defining the specifics of the rule."	Open Information Security Foundation (2025): Suricata Rules
test access point	"a device used to monitor and analyze network traffic without disrupting the normal operation of the network. It is typically placed between two Ethernet devices and operates transparently,	Hilscher (n.d.): Test Access Point (TAP)

	allowing it to capture and mirror all the data passing through the connection."	
tools for collecting network flow data	"Network flow monitoring systems provide means for extraction of network flow information from network traffic. Some of the systems also help in basic analysis of network flows, including bandwidth level, protocol usage and IP addresses involved in communication."	ENISA (2020): Measures for proactive detection of incidents, GitHub
Traffic Light Protocol	"a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s)."	U.S. Cybersecurity and Infrastructure Security Agency (2022): Traffic Light Protocol (TLP) Definitions and Usage
YARA rules	"YARA rules are malware detection patterns that are fully customizable to identify targeted attacks and security threats specific to [an] environment"	Trend Micro (n.d.): YARA Rules

Annex V: List of abbreviations

Abbreviation	Full Name
ACSC	Australian Cyber Security Centre
AfricaCERT	African Forum of Computer Emergency Response Teams
AIVD	Dutch General Intelligence and Security Service
APCERT	Asia Pacific Computer Emergency Response Team
APT	Advanced Persistent Threat
AUC	African Union Commission
BSI	German Federal Office for Information Security
BSOC	Federal Security Operations Centre
CADS	Cyber Analytics and Data System
CCB	Cyber capacity-building
CERT	Computer Emergency Response Team
CERT-Bund	Federal Computer Security Incident Response Team of Germany
CI	Critical infrastructure
CIRCL	Computer Incident Response Center Luxembourg
CIS	Center for Internet Security
CISA	United States Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer

CMM	Cybersecurity Capacity Maturity Model
CNMF	United States Cyber National Mission Force
CSF	Cybersecurity Framework
CSIRTs	Computer Security Incident Response Team
CSOA	Cyber Solidarity Act
CSPM	Cloud security posture management
CTI	Cyber threat intelligence
CVE	Common Vulnerabilities and Exposures
DaaS	Detection-as-a-service
DNS	Domain Name System
DoD	United States Department of Defense
DORA	Digital Operational Resilience Act
EDR	Endpoint Detection and Response
eGA	e-Governance Academy
ENISA	European Union Agency for Cybersecurity
EPF	European Peace Facility
FCEB	Federal Civilian Executive Branch
FIRST	Forum of Incident Response and Security Teams
G7	Group of Seven
GGE	Group of Governmental Experts
HBC	Host Based Capability
HFO	Hunt forward operations
IADB	Inter-American Development Bank
ICTs	Information and communications technologies
IDS	Intrusion detection systems
IoCs	Indicators of compromise
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITZBund	Federal Information Technology Centre
JICA	Japan International Cooperation Agency
JPCERT/CC	Japan Computer Emergency Response Team Coordination Center
KEVs	Known exploited vulnerabilities
LLMs	Large language models

LME	Logging Made Easy
LOTL	Living off the land
MISP	Open Source Threat Intelligence and Sharing Platform
MIVD	Dutch Military Intelligence and Security Service
MS-ISAC	Multi-State Information Sharing and Analysis Center
MTTD	Mean time to detect
NCAs	National cybersecurity authorities
NCPS	National Cybersecurity Protection System
NCSC	Dutch/UK National Cyber Security Centre
NDN	National Detection Network
NIS 2	Directive on measures for a high common level of cybersecurity across the Union (2022)
NIST	United States National Institute of Standards and Technology
NorCERT	Norwegian CERT
OIC-CERT	Organisation of The Islamic Cooperation Computer Emergency Response Teams
OT	Operational technology
PaCSON	Pacific Cyber Security Operational Network
SAOs	Suspicious activity observations
SCS	Shared Cybersecurity Services
SIEM	Security Information and Event Management
SLTT	State, Local, Tribal, and Territorial
SMEs	Small and medium-sized enterprises
SOAR	Security Orchestration, Automation, and Response
SOCaaS	SOC-as-a-Service
SOC	Security Operations Centre
SOPs	Standard Operating Procedures
TAP	Test Access Point
TF-CSIRT	Task Force CSIRT
TLP	Traffic Light Protocol
TTPs	Tactics, techniques, and procedures
UN	United Nations
UNIDIR	UN Institute for Disarmament Research
UN OEWG	UN Open-Ended Working Group on the security of and in the use of information and communications technologies

WID	Warn- und Informationsdienst
XDR	Extended detection and response

Acknowledgments

This analysis was supported by the working group “Technical Capabilities for Norms Implementation” and experts through interviews, a workshop held in Berlin in May 2025, and online collaboration. The views and opinions expressed in this paper are those of the author and do not reflect the official policy or position of the experts or of their respective employer/s.

In alphabetical order, acknowledging essential contributions of:

1. Klée Aiken, Forum of Incident Response and Security Teams
2. Joel Aleburu
3. Robert Collett
4. Samuele Dominioni
5. Andrew Dwyer, Royal Holloway, University of London
6. Tod Eberle, The Shadowserver Foundation
7. Vera Ezeanolue
8. Chris Gibson, Forum of Incident Response and Security Teams
9. Richard Harris
10. Max Heinemeyer
11. Eve Hunter, Detecon International GmbH
12. Sophia Klumpp
13. Koichiro Komiyama, JPCERT/CC
14. Lisa Lobmeyer, Security Research Labs
15. Klara Marland
16. Jiro Minier, DCSO
17. Takumi Nakano, JPCERT/CC
18. Melanie Niethammer
19. Alexandra Paulus, German Institute for International and Security Affairs (SWP)
20. Mark Peters
21. Daniel Sauder
22. Berenike Vollmer
23. Fee-Marie von der Brelie

At interface, the author would particularly like to thank Sven Herpig for input and advice along the way, Jasen Ho for research support, Luisa Seeling for support in

editing the text, Alina Siebert for layouting the paper and designing the paper's visuals, Helene Pleil for constructive feedback on a first draft, Iana Pervazova for helping to spread the word about this publication, and Frederic Dutke and Nicole Lemke for support in implementing the workshop.

This project was made possible by the generous support of the German Federal Foreign Office. The views expressed in this paper do not represent the official position of the ministry.

Author

Christina Rupp
Senior Policy Researcher Cybersecurity Policy and Resilience
crupp@interface-eu.org
+49308145037880

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
c/o Publix
Hermannstraße 90
D-12051 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com