Research Paper

International Security Programme

June 2024

A principles-based approach to cyber capacity-building (CCB)

Understanding and operationalizing the OEWG CCB principles

Joyce Hakmeh, Amrit Swali and Robert Collett

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

Summary

- Cyber capacity-building (CCB) enables states to stay abreast of technological advancements and safeguard critical infrastructure against evolving cyberthreats. Adopting a principles-based approach to CCB can enhance efficiency, effectiveness and collaboration through the standardization of practices and the promotion of responsible state behaviour in these endeavours.
- In 2021, under the UN Open-ended Working Group on security of and in the use of information and communications technologies (hereafter, OEWG), UN member states agreed to 10 capacity-building principles to guide CCB activities. The principles have the potential to maximize the efficient and responsible deployment of CCB activities, and standardize them. However, effective operationalization of the CCB principles depends on implementers having a clear and thorough understanding of what they mean.
- Recognizing the foundational and enabling nature of CCB, OEWG stakeholders (both state and non-state) have called for greater comprehension and integration of the principles as a way of facilitating responsible state behaviour in cyberspace.
- While this paper focuses on the OEWG's CCB principles, it is intended to support broader efforts aimed at adopting a principles-based approach to CCB. Effective CCB requires the proactive engagement of a range of actors, not just states, to ensure that principles are applied appropriately and adapted to the rapidly evolving cyber landscape.

Introduction

Cyber capacity-building (CCB) is 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). This field of cooperation has evolved over approximately two decades and involves a diverse ecosystem of stakeholders – including technical incident responders, law enforcement agencies and civil society actors – actively engaged in its development, delivery and ongoing evaluation.[1] This collaborative environment underscores the collective efforts required by a broad range of stakeholders to effectively deliver CCB activities and navigate the evolving challenges and opportunities in cyberspace.

In 2021, the United Nations (UN) Open-ended Working Group (OEWG) on developments in the field of ICTs in the context of international security – a platform that includes all UN member states and aims to address issues related to the international security dynamics of ICTs – issued a final consensus report in which it outlined 10 principles to guide CCB efforts in this context (Figure 1).[2] Since then, OEWG member states and other stakeholders have emphasized the need for a better understanding of those principles and guidance on how to mainstream them in CCB activities.[3] Indeed, the OEWG's second annual progress report in 2023 recommended the development of 'voluntary checklists and other tools to assist States in mainstreaming the capacity-building principles from the 2021 OEWG report into capacity-building initiatives related to ICT security'.[4]

This paper responds to these ongoing calls within the OEWG to raise awareness of the CCB principles and to enhance understanding of their purpose, utility and application. In the following three sections, this paper situates the CCB principles within the framework of responsible state behaviour and contextualizes them in international development, explores what the principles mean and entail, and then provides a project example to illustrate their practical application. While

---

1 Collett, R. (2021), 'Understanding cybersecurity capacity building and its relationship to norms and confidence building measures', *Journal of Cyber Policy*, 6(3), pp. 298–317, https://doi.org/10.1080/23738871.2021.1948582.

2 United Nations General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

3 European Union statement to the OEWG (2024), 'Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025: Key EU messages for agenda item: capacity building', https://estatements.unmeetings.org/estatements/12.1255/20240307150000000/I9KvsxrRpaNy/z367AnqDwcym_en.pdf.

4 UN OEWG (2023), 'Second annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025 submitted to the 78th session of the general assembly pursuant to general assembly resolution 75/240', July, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_26_July_2023.pdf.

the paper focuses on the OEWG CCB principles, it is intended to support broader efforts aimed at adopting a principles-based approach to capacity-building. Further research is needed on how different stakeholder groups can operationalize the CCB principles and how they can be applied in other CCB projects. As such, this paper is an initial step in a long-term journey.

Figure 1. The OEWG's 10 cyber capacity-building principles

Process and purpose	Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
	Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
	Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
	Capacity-building should be undertaken with full respect for the principle of State sovereignty.
	Access to relevant technologies may need to be facilitated.
Partnerships	Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.
	As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
	The confidentiality of national policies and plans should be protected and respected by all partners.
People	Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.
	The confidentiality of sensitive information should be ensured.

Source: United Nations General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Scope and methodology

Section 1 of this paper highlights the critical role CCB plays in empowering states to leverage ICTs for economic development and security, making the case for a principles-based approach to standardize efforts, prevent misuse, and ensure effective and equitable implementation. Section 2 considers each of the 10 OEWG CCB principles, extracting key terms, exploring their meanings and outlining the contribution of each principle to international peace and security. Additionally, this section examines the interconnections between each principle, advancing a comprehensive understanding of how they work together and how different

stakeholders should interpret them. Section 3 presents a project example focused on establishing a national point of contact for the OEWG points of contact (POC) directory and improving cyberthreat intelligence-sharing capabilities within a national computer security incident response team (CSIRT). It provides illustrative suggestions for how a principles-based approach might be applied in the design, implementation and evaluation phases of the project. This paper is aimed primarily at the stakeholders of the OEWG,[5] which include all UN members, civil society actors and private sector representatives, in response to a recommendation that member states agreed to in 2023.[6] In addition, the paper is intended to socialize the OEWG's CCB principles among the broader CCB community, and promote the benefits of a principles-based approach to CCB to all actors involved in this ecosystem.

5 For illustrative purposes, refer to this OEWG webpage featuring submissions from various stakeholders: UN Office for Disarmament Affairs (undated), 'Open-Ended Working Group on Information and Communication Technologies', https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=author_type_documents_%3ANon-governmental%20organization.
6 See footnote 4.

Section 1. A principles-based approach to CCB

CCB has garnered increased attention for its role in empowering all countries to harness the benefits of ICTs, mitigate the risks associated with their use and prepare for the integration of new and emerging technologies. While CCB activities – such as training, policy development, collaboration and technical support – help build national resilience, they also facilitate the enhanced cooperation needed between countries to address transnational cyberthreats, including those that threaten international peace and security.

Besides achieving better security, CCB activities drive digital empowerment and innovation, all of which are essential for achieving the UN's Sustainable Development Goals (SDGs).[7] By equipping states with the necessary knowledge and skills, CCB helps reduce the digital divide and ensures secure and equitable access to technological advancements.

The 2021 report of the OEWG emphasizes this enabling role of CCB and underscores its importance in facilitating the meaningful participation of developing states in ICT negotiations and discussions, as well as strengthening their capacity to address vulnerabilities in their critical infrastructure. The report highlights how CCB can enhance the resilience and security of states by developing skills, human resources, policies and institutions, enabling them to fully benefit from digital technologies.[8] The ongoing OEWG continues to prioritize CCB as a key driver for responsible state behaviour in cyberspace.

Given the central role that CCB plays in achieving national prosperity, fostering stability in cyberspace, and maintaining international peace and security, it is paramount that CCB activities are effective, efficient and equitable. This is especially important as the demand for CCB increases. This paper argues that adopting a principles-based approach to CCB can help achieve these objectives

7 United Nations Department of Economic and Social Affairs (undated), 'The 17 Goals', https://sdgs.un.org/goals.
8 UN General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*.

by standardizing efforts, ensuring optimal resource utilization and safeguarding against unintended consequences and the potential misuse and/or abuse of CCB activities – all of which contributes to the overarching goals of prosperity, stability and security in cyberspace.

A principles-based approach to international cooperation or collaboration is not new. The OEWG principles build on a rich history of cooperation in international development,[9] particularly the 2011 principles of effective development cooperation (also known as the Busan principles).[10] They also build on the Global Forum on Cyber Expertise's (GFCE) principles included in the 2017 Delhi Communique, which in turn were inspired by the Busan principles.[11] While the Busan and the GFCE's principles have different framings that reflect their unique contexts, they share foundational elements and common themes including: the national ownership of development priorities; a focus on results, partnerships, inclusion, respect for rights and transparency; and accountability. These themes also feature prominently in the OEWG principles, firmly establishing linkages between CCB and the international development field.

In the international development field, principles have helped to standardize, guide and inform activities so that they are effective, ethical and sustainable. The same objectives are sought in CCB through the OEWG principles, which provide an opportunity to streamline CCB efforts and establish a common understanding of best practice. While these principles are not legally binding, they represent a unanimous agreement among all OEWG member states that CCB is a significant priority. Recognized as a critical, enabling and cross-cutting pillar of the framework for responsible state behaviour, CCB aims to increase resilience against cyberthreats and promote responsible behaviour in cyberspace. Adopting a principles-based approach to CCB can enhance the resilience and security of states, allowing them to fully benefit from digital technologies and supporting their roles as responsible players in cyberspace, thereby contributing to international peace and security. However, to effectively adopt and apply these principles, a thorough understanding of their individual and collective meanings is essential.

Furthermore, a principles-based approach to CCB can help safeguard against the misuse and abuse of CCB activities, and the capabilities that are developed as a result of these activities. As a form of international development, CCB aims to level the playing field among states and address inequities in global capacities and capabilities. To this end, some CCB activities might involve the transfer of tools and skills that can be used for both beneficial and harmful purposes. Intentional misuse could involve using these tools and skills for oppressive activities, such as the improper use of surveillance technologies by law enforcement agencies, thereby violating human rights and fundamental freedoms. Unintentional misuse could occur through the provision of tools and techniques without adequate training, oversight or regulatory

9 See Annex A for a list of principles frameworks relevant to CCB.
10 Global Partnership (undated), 'Global Partnership for Effective Development Co-operation', https://www.effectivecooperation.org.
11 Global Forum on Cyber Expertise (2017), 'Delhi Communique on a GFCE Global Agenda for Cyber Capacity Building', Global Forum on Cyber Expertise, https://thegfce.org/wp-content/uploads/DelhiCommunique-1.pdf.

protections. Additionally, there is a risk that CCB could reinforce harmful international political power dynamics, potentially hindering the equitable transfer of skills, expertise and knowledge. A principles-based approach, particularly one that is depoliticized, evidence based and results focused, can help mitigate these risks, encouraging equity in the global CCB ecosystem and contributing to international peace and security.

The OEWG CCB principles are an important milestone agreed upon by all states and they serve as a cornerstone in guiding CCB activities. However, their effective operationalization hinges on their being clearly understood. Section 2 considers each of the 10 principles and explores the interconnections between them.

Section 2. Understanding the OEWG's CBB principles

Each of the 10 OEWG principles embodies a specific purpose, while playing a contributory role within the CCB ecosystem. The factsheets in this section look at the principles primarily from a state perspective, reflecting the state-led nature of the OEWG and its report, and the responsibility of states to foster a collaborative and accountable CCB ecosystem. Where appropriate, however, responsibilities and roles for non-state actors are also considered.

The 10 principles are not legally binding, but their adoption in 2021 represents – and speaks to the need for – an important standardizing function. The analysis presented here found that the principles can complement, align with and support each other. In some cases, there can also be tension between them. It is incumbent upon states and non-state actors to ensure that any tension between principles is dealt with appropriately and in a way that does not jeopardize international peace and security.

Through 10 factsheets, this section explores the principles, both as individual and collective guidance. The factsheets highlight the key terms in each principle, explore what these terms mean, outline how each principle contributes to international peace and security, and then considers how the principle works with other principles. In doing so, these factsheets encourage policymakers and practitioners to understand each principle on its own merit and consider how the principles can work together to contribute to a global CCB ecosystem.

Crucially, the interpretation presented in the factsheets is not the only way to perceive or understand the principles. A practical understanding (and subsequent application) of the principles will occur in a context, so the interpretation of the principles must be context-specific. The interpretation presented in this section is intended as a baseline that should be context-dependent and should evolve

as understanding and definitions of key international concepts develop. It is also intended as an international interpretation, rooted in globally recognized definitions that can garner consensus at a broad level.

Methodology

These factsheets are the result of an analytical exercise that sought to understand the component parts of each principle and how they create a cohesive and cross-cutting narrative.

This exercise included analysing each principle across five areas, which informed the design, presentation and content of the factsheets:

1. **Audience:** the CCB principles were created in a forum for UN member states and are primarily designed to guide state behaviour. However, the responsibilities and concepts they engender must be differentiated to suit the ecosystem of (state and non-state) actors involved in CCB. In some cases, the way a state should interpret a principle will differ depending upon whether they are funding an activity (traditionally described as a 'donor' country) and/or whether they are a beneficiary of it. In this part of the exercise, the authors sought to understand the principle firstly from the perspective of state actors and then from the perspective of appropriate non-state actors.
2. **Language and interpretation:** several principles combine concepts and terminology from different fields of practice, including programme management, international relations, international security and international development. Through research, analysis and consultations with OEWG stakeholders, the authors identified the key terms or phrases within each principle, analysed them as separate component parts and then formulated a connection between these terms and phrases to understand how they contributed to the principle's ultimate purpose or role. The interpretation of the key terms and phrases build on existing literature and analysis, and have been interpreted and understood through the lens of internationally recognized definitions. Where appropriate, references are included; however, the interpretation of the terms is largely determined by the authors based on the application of certain international definitions to CCB as a field and the principle itself.
3. **Drivers:** to better understand the role of the principles, this part of the analysis considered what each principle's direct or immediate purpose within the CCB ecosystem would be. The OEWG categorizes the 10 principles into three groups: process and purpose; partnerships; and people. Across these three groups, the authors identified four overlapping 'drivers': efficacy; ethics and values; peace and security; and political motivations or priorities. Principles from each of the OEWG's three groups embody elements of these drivers: for example, while there are only five principles under 'process and purpose', almost all of the 10 principles contribute to ensuring CCB is effective.

4. **Objective:** the ultimate objective of the OEWG is to contribute to international peace and security, which is captured in paragraph 54 of the OEWG's 2021 report: 'benefits of capacity-building […] contribute to building a more secure and stable ICT environment'. Importantly, while CCB contributes to this ultimate goal, it can also achieve objectives and impacts beyond this. As outlined in paragraph 54, these 'benefits' – or broader objectives – include: to 'prevent or mitigate the impact of malicious ICT activity'; 'facilitate genuine participation in discussions on ICTs in the context of international security'; 'address vulnerabilities in their critical infrastructure'; 'develop the skills, human resources, policies and institutions that increase resilience and security of States'; 'promot[e] adherence to international law and the implementation of norms of responsible state behaviour'; 'support […] the implementation of CBMs' and 'ensur[e] an open, secure, stable, accessible and peaceful ICT environment'.[12] These intermediate objectives are more easily extracted from the principles individually, demonstrating how achieving the OEWG's ultimate objective is reliant on working towards (through all four pillars of the framework of responsible state behaviour) facilitating or enabling objectives. This part of the analysis sought to match the principles with the intermediate objectives noted in paragraph 54 of the 2021 OEWG report.
5. **Relationship with other principles:** as discussed above, the principles should not be seen in isolation. While they embody an individual purpose or role, they interact with, complement and support each other, and there can be tension between them. For example, CCB is more results focused (Principle 2) if it is evidence-based (Principle 3). In this part of the analysis, the authors sought to better understand how the principles should be viewed as part of a greater whole and how the principles work with each other. Crucially, this part of the analysis does not consider every type of relationship between the principles; instead, the analysis focuses on those relationships and interactions between principles that are most critical in the operationalization of principles.

The results from this exercise were then tested in two workshop consultations held on the margins of the OEWG sessions. The first consultation, held on 24 July 2023 during the fifth session of the current OEWG, sought to better understand how the CCB principles should be interpreted and applied. The consultation brought together 30 participants from various countries and non-state organizations, and used scenario-based discussions to consider how and when principles might apply to a specific CCB situation and how they can help prevent CCB being misused or abused.

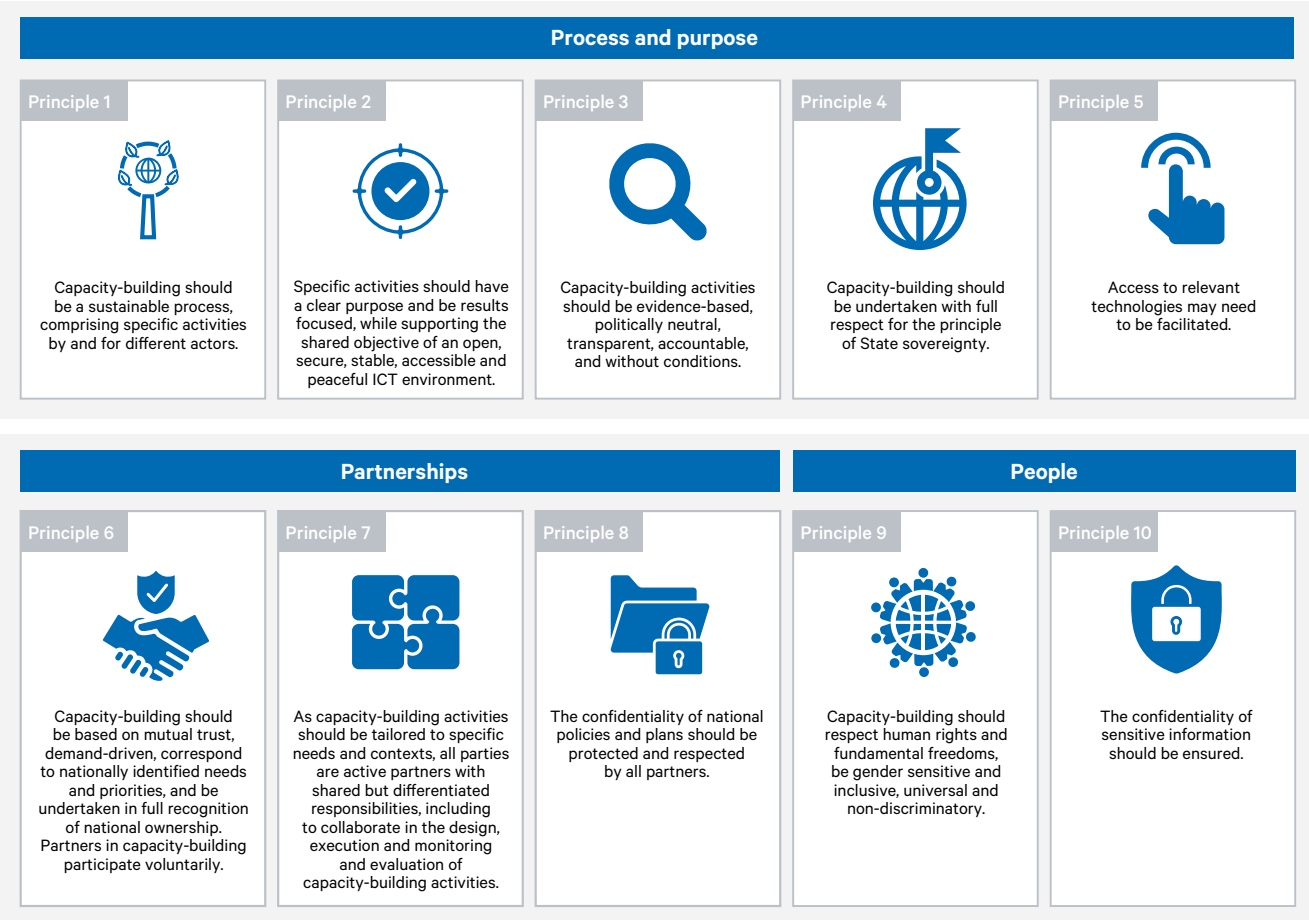
The second consultation, held on 6 March 2024 during the seventh session of the current OEWG, sought to test the authors' analysis of the principles. In a similar format to the first consultation, this second consultation brought together 30 participants from member states and non-state organizations and encouraged them to think critically about what the principles mean.

Finally, these factsheets have been strengthened by peer review and feedback from the project's Advisory Group.

---

12 UN General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*.

Figure 2. OEWG CCB principles



Source: United Nations General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*.

1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.

Sustainability in cyber capacity-building refers to the creation of a global, viable and long-lasting CCB ecosystem. There are broadly two dimensions to ensuring that CCB is a **sustainable process**. The first relates to the sustainability of benefits and successes after the activity is complete. The second is that CCB should meet present needs 'without compromising the ability of future generations to meet their own needs'.* The consideration of future generations' needs should include, but not be limited to, the climate and environmental impact of CCB.† Sustainable CCB is more likely to have a positive long-term impact and can help ensure the efficiency and responsible use of resources in CCB activities.

By and for different actors emphasizes the multi-stakeholder nature of cyber capacity-building. The design and implementation of CCB requires a variety of actors (both state and non-state) for their different skills, resources and perspectives. Furthermore, capacity-building should be for different actors because its benefits extend beyond government to citizens, civil society and the private sector.‡

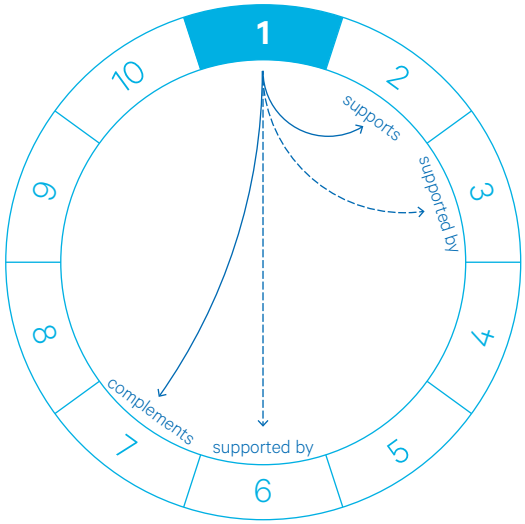
* Brundtland Commission (1987), *Report of the World Commission on Environment and Development: Our Common Future*, United Nations, https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf.
† World Bank (2023), *Green Digital Transformation: How to Sustainably Close the Digital Divide and Harness Digital Tools for Climate Action*, Climate Change and Development Series, Washington, DC: World Bank, http://hdl.handle.net/10986/40653.
‡ Ciglic, K. and Hering, J. (2022), 'A multi-stakeholder foundation for peace in cyberspace', *Journal of Cyber Policy*, 6(3), pp. 360–374, https://doi.org/10.1080/23738871.2021.2023603.

How does this principle help achieve international peace and security?

Sustainability is a matter of international peace and security, both in terms of the environment and resource management, and in terms of supporting global development. Acknowledging the role of a wide variety of actors ensures that responsibility, accountability and ownership is shared and felt among all relevant stakeholders.

This principle helps achieve international peace and security by establishing CCB as a global, interconnected endeavour with shared aims and motivations between states.

How does this principle work with other principles?



Principle 1 **supports** Principle 2, because the sustainability element is intrinsically linked to results.

Principle 1 is **supported by** Principle 3 because evidence and accountability underpin sustainability. It is also **supported** by Principle 6, because results are more likely to be sustained when states are able to feel ownership over and responsible for the long-term success of CCB.

Principle 1 also **complements** Principle 7 through its emphasis on the multi-stakeholder nature of CCB.

2

Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.

While CCB is generally a positive endeavour, it can be misused or have unintended consequences. To mitigate these risks, CCB activities should be **specific** and have a **clear purpose**: i.e. goals should be clearly defined. This contributes to the efficient use of resources and better outcomes.

Emphasizing the **shared objective of an open, secure, stable, accessible and peaceful ICT environment** firmly aligns CCB activities with the framework for responsible state behaviour in cyberspace and highlights the importance of CCB in achieving this objective.* This 'shared objective' ensures equitable access to digital technologies and ICTs and reduces the risk of the militarization and fragmentation of cyberspace.

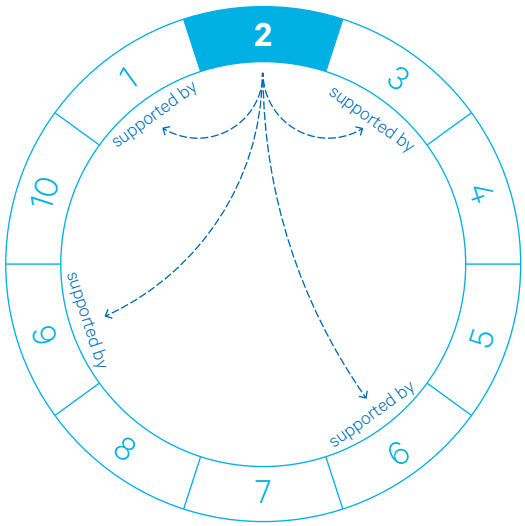
CCB that is **results focused** prioritizes achieving measurable benefits, especially for the partner country. By focusing on results, it is easier to demonstrate the value of CCB activities and learn lessons for future activities. Focusing on results can also help ensure that CCB is driven by a purpose, minimizing the risk of nefarious or unintended use.

* UN General Assembly (2021), 'Open-ended working group on developments in the field of information and telecommunications in the context of international security'.

How does this principle help achieve international peace and security?

This principle underscores the ultimate motivation of the OEWG: to work towards international peace and security. The less cyberspace is militarized, and the more intentional capacity builders can be about their activities, the more open, secure, stable, accessible and peaceful cyberspace will be. By ensuring that CCB activities, projects and interventions are clear on the outcome and purpose, this principle protects and encourages intentional and deliberate CCB, contributing to overall security by minimizing inadvertent risks.

How does this principle work with other principles?



The focus on results is **supported by** an emphasis on sustainability (Principle 1) and evidence-based approaches (Principle 3). All of these elements are crucial to having a clear goal.

An open, secure, stable, accessible and peaceful ICT environment is **supported by** transparency and accountability in capacity-building (Principle 6). Similarly, the *open* and *accessible* components of the shared objective are **supported by** inclusion and respect for human rights and fundamental freedoms (Principle 9), all of which are key elements of a global cyberspace.

3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.

Capacity-building is **transparent** when all (relevant) observers can see what CCB activity is occurring and for what purpose(s). Transparency is linked to and enables **accountability**. Facilitating transparency and accountability requires clear communication and openness among all actors. Prioritizing transparency and accountability can build trust and foster a more positive collaborative environment among CCB stakeholders.

An **evidence-based** approach to CCB is one where activities are informed by data, research and lessons learnt from previous initiatives. Evidence should include knowledge of the local context, thereby contributing to activities that are sensitive and responsive to local needs and conditions.

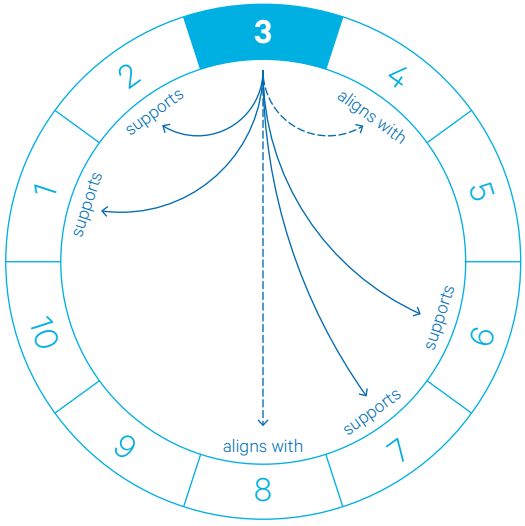
This principle is designed to sustain political momentum for CCB across subsequent governments and among stakeholders, but it also protects CCB against bias and politicization. A **politically neutral** approach to capacity-building helps ensure that CCB is not used for (geo)political purposes and is guided by objective and impartial considerations.

Stipulating that CCB is **without conditions** contributes to political neutrality by ensuring that CCB is done for the right reasons. However, it is important to distinguish between political conditionality and programmatic conditionality: programme-related conditions (e.g. party A agrees to deliver a CCB activity if party B agrees to sustain the results) may nonetheless be necessary to apply other principles and would not contravene the spirit of Principle 3.

How does this principle help achieve international peace and security?

CCB should reduce digital divides and facilitate global participation in cyberspace: both are important for levelling the playing field and stabilizing international peace and security. This principle helps achieve international peace and security by de-politicizing CCB and discouraging its use to influence other countries' domestic and international politics. The emphasis on transparency reduces the risk of tension arising from a misunderstanding of other countries' CCB activities.

How does this principle work with other principles?



The evidence-based approach in this principle **supports** a focus on sustainability (Principle 1) and measurable results (Principle 2). The emphasis on transparency and accountability **supports** national ownership (Principle 6) and effective partnerships (Principle 7) by allowing actors to feel ownership over activities.

Political neutrality and capacity-building without conditions **aligns with** respect for state sovereignty (Principle 4) and the confidentiality of national plans (Principle 8).

4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.

State sovereignty is enshrined in the United Nations Charter* and it is incumbent upon all member states to adhere to this principle. CCB interventions can be intrusive and exposing, and the risk of infringing on state sovereignty is high if appropriate safeguards and limitations are not put in place and respected.

Sovereignty would be infringed by a CCB activity if it compromised a state's political independence. The risk of state sovereignty being infringed is greater for a country receiving assistance; as such, respect for their agency and national ownership of the CCB is essential for ensuring this principle is applied.

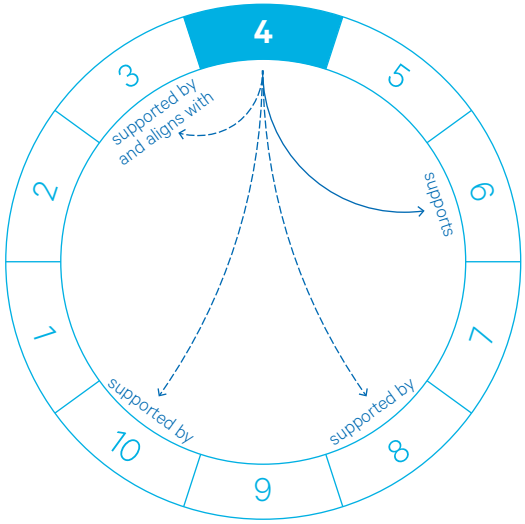
Respect for state sovereignty also includes the recognition of a state's right to participate as an equal actor in a global system. All states have a responsibility to facilitate and encourage behaviour in cyberspace that does not infringe upon sovereignty – and this responsibility is greater for those states with more developed cyber capabilities. Where appropriate, sovereignty also implies responsibilities under international law and norms.

* 'Organization is based on the principle of the sovereign equality of all its Members.' – UN (undated), 'Charter of the United Nations, Article 2(1)'.

How does this principle help achieve international peace and security?

State sovereignty is central to international relations and the UN Charter: it is a principle designed to protect the agency of all states so that they can contribute to global governance and development with independence and respect. Respecting state sovereignty is vital for achieving international peace and security. This principle codifies the need for equality among states.

How does this principle work with other principles?



Principle 4's respect for state sovereignty **supports** the national ownership of capacity-building as outlined in Principle 6, recognizing a state's agency in CCB.

Principle 4 **aligns with** CCB being politically neutral and without conditions (Principle 3), recognizing states as equals.

Implementers must carefully consider all phases and forms of CCB activity. The act of assessing contexts, determining needs, sharing tools and resources, and implementing and delivering CCB interventions risk infringement of sovereignty if not done with full transparency and respect for the partner state. As such, transparency and accountability (Principle 3) **support** Principle 4, and Principle 4 is supported by confidentiality (Principles 8 and 10).

5 Access to relevant technologies may need to be facilitated.

In accordance with the role of CCB in developing the 'skills, human resources, policies, and institutions' of all states,* some CCB activities will benefit from a party having **access to relevant technologies**, which might consist of hardware, software or both. This can help empower individuals and organizations to navigate the evolving cyber landscape, defend against cyberthreats, participate in discussions on ICTs and contribute to the overall resilience of the digital ecosystem. Often, a state's political and strategic needs can influence what type and level of CCB it offers, which can sometimes cause states to dismiss the need for technologies. **Access to relevant technologies** can help level the playing field between states.

Here, access need not be limited to physical or electronic access, but could also encompass having the necessary skills, knowledge and tools to maintain and use a particular technology. Whether a particular technology is relevant and appropriate for a CCB activity will depend upon the nature of the activity, the context and considerations derived from the other principles. For this reason, this principle stresses that access ***may*** need to be facilitated rather than *should* be facilitated in all circumstances.

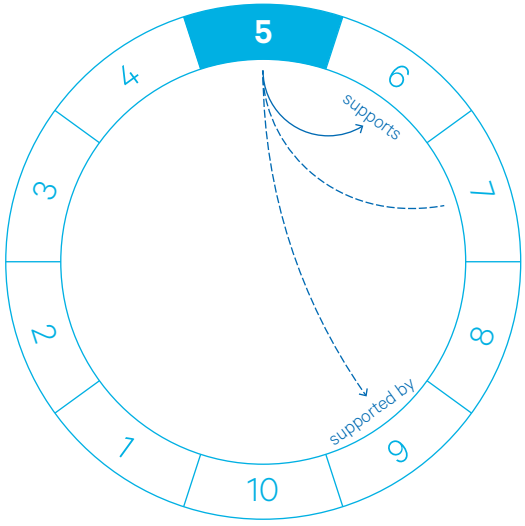
* UN General Assembly (2021), *Open-ended working group on developments in the field of information and telecommunications in the context of international security*.

How does this principle help achieve international peace and security?

Facilitating access to technology can narrow the digital divide and increase global cybersecurity readiness. It can help build states' long-term resilience and empower them to deal with cyberthreats. In turn, this can help achieve international peace and security by ensuring all states are equipped to deal with these threats, nationally and internationally.

However, to achieve this, it is necessary to consider the purpose of the CCB activity, and the need to apply other principles.

How does this principle work with other principles?



By recognizing that there might be a need to facilitate access to relevant technologies, Principle 5 **supports** a demand-driven approach to capacity-building and national ownership (Principle 6).

This principle must be read in conjunction with others, namely Principle 7 and Principle 9, to minimize tensions. Any access to technologies must be justified by needs and context (Principle 7), and the potential of any human rights risks (Principle 9) arising from the technology use must be considered.

6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.

A country receiving CCB should have **national ownership** over the activity. This involves taking a leading role in its direction and ensuring alignment with **nationally identified needs and priorities**. CCB that demonstrates these features can be described as **demand-driven**, where partner countries play a significant role in determining the CCB they receive according to their domestic development agendas.* Government leadership is necessary for applying this principle, but there is a role for non-state actors.

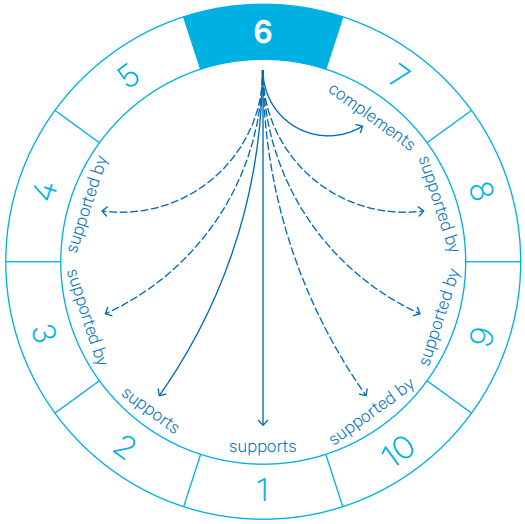
Partners in capacity-building **participate voluntarily** when they are empowered to make a free, un-coerced and informed decision about whether to join or stay in a CCB partnership. All partners should participate based on and according to their means. This contributes to partnerships based on **mutual trust**, which underpins strong collaboration.

* Bandura, R. and Hammon, M. (2019), 'A demand driven approach to development: A CSIS Primer', Center for Strategic and International Studies (CSIS), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190515_BanduraHammondRunde_DemandDriven_WEB.pdf.

How does this principle help achieve international peace and security?

This principle supports international peace and security by emphasizing national ownership and mutual trust in CCB. In turn, this fosters productive and constructive international partnerships that contribute positively to a global CCB ecosystem that recognizes the agency of all actors.

How does this principle work with other principles?



The ideas in this principle (e.g. *demand-driven, identified needs and priorities*) **support** sustainability (Principle 1). This principle also supports Principle 2 by focusing on national needs to guarantee results. Voluntary participation **complements** the need for active partnerships in Principle 7, where all actors recognize their roles and responsibilities.

National ownership is **supported by** neutrality, accountability and transparency (Principle 3), respect for state sovereignty (Principle 4) and respect for confidentiality (Principle 8). Both mutual trust and national ownership are **supported by** an inclusive approach and ensuring the protection of sensitive information (Principles 9 and 10): all parties should be able to trust that partners respect these principles.

7

As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.

'All parties are active partners' refers to the need for equitable partnerships in CCB. This implies a multi-stakeholder approach and promotes fluid exchanges of knowledge and triangular cooperation between actors, while discouraging top-down, one-size-fits-all approaches. Alignment between partners increases buy-in and harnesses a wider range of experiences, perspectives and resources. This helps to ensure that CCB is **tailored to specific needs and contexts**, not to countries, protecting against politicization.

This principle is based on a similar concept in international development that recognizes the importance of sharing responsibilities in a way that is equitable and reflects global realities.* **'Shared but differentiated responsibilities'** acknowledges that countries differ in what they bring to CCB and to global cybersecurity.† This principle recognizes the power disparity between CCB actors but advocates for agency that encourages actors to play to their own strengths.

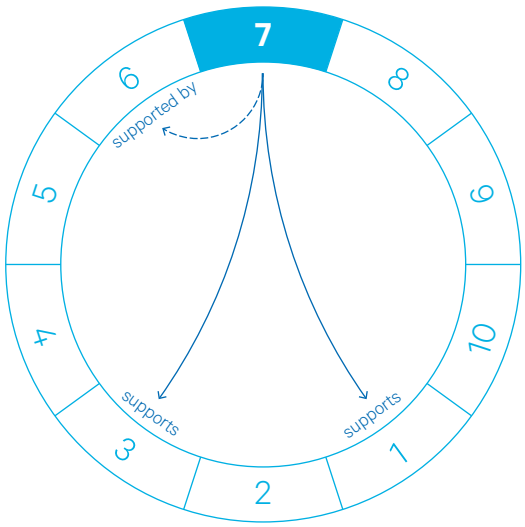
* Calderaro, A. and Craig, A. J. S. (2020), 'Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity-building', *Third World Quarterly*, 41(6), pp. 917–938, https://doi.org/10.1080/01436

† The phrase is similar to 'common but differentiated responsibilities' – a central concept in The United Nations Framework Convention on Climate Change (1992) 597.2020.1729729.

How does this principle help achieve international peace and security?

By identifying shared but differentiated responsibilities, this principle stresses that all actors can and should contribute to CCB. In doing so, this principle can help achieve international peace and security by framing CCB as a global endeavour and ensuring that responsibility and expectations are shared proportionately, allowing actors to contribute to global security in a way that is appropriate for them.

How does this principle work with other principles?



A partnership-based approach **supports** achieving sustainable results (Principle 1) because it appropriately shares responsibility and accountability.

A partnership-based approach **supports** neutrality, accountability and transparency, reducing the risk of CCB being politicized (Principle 3).

The partnership-based approach in this principle is **supported by** voluntary participation (Principle 6).

8 The confidentiality of national policies and plans should be protected and respected by all partners.

In some CCB activities, **national policies and plans** may need to be shared or made readily available. Many national policies and plans relevant to CCB will already be public but, where they are not, their **confidentiality** should be **protected and respected**. Confidentiality depends upon a chain and range of responsibilities – from classification to handling – that all parties have a role in. As such, it is incumbent upon all partners to protect any sensitive information relating to national matters of government, especially those related to security.

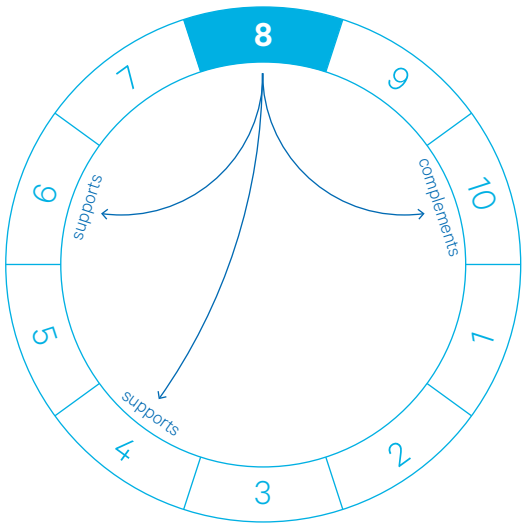
Respecting the confidentiality of national plans contributes to a more extensive exchange of sensitive information, enabling better design, risk management, and monitoring and evaluation. **Protected and respected** can be interpreted as a strong encouragement to states to treat other nations' policies and plans in the same way they would want their own to be treated. Sharing national policies and plans is inherently a state–state collaboration, but **all partners** should uphold this principle.

Implicitly, this principle acknowledges that a core part of CCB is learning from the experiences of other states. In a CCB partnership, sharing national plans and policies ensures that activities can be collaborative and iterative, and that lessons learnt can be integrated, benefiting all actors involved.

How does this principle help achieve international peace and security?

Respect for the confidentiality of national policies and plans builds trust between partners in the international system and reduces the security and diplomatic risks that may arise from information leaks.

How does this principle work with other principles?



By protecting the confidentiality of national plans, Principle 8 **supports** a respect for state sovereignty (Principle 4). It also ensures mutual respect between states and builds mutual trust (Principle 6).

Principle 8 **complements** Principle 10 as both relate to confidentiality but can be understood to address different types of sensitive information: the former concerns national policies and the business of government, the latter the personal data of individuals.

9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.

Gender sensitive and inclusive CCB activities are cognizant of the context's gender dynamics at political, institutional and socio-economic levels, and the intervention's gendered impact(s). Gender-sensitive design will seek evidence of gendered dynamics to inform activity design and challenge gendered assumptions. Inclusive design will ensure diverse participation.* Capacity-building is **universal** when there are no permanent roles and all stakeholders can participate in and benefit from it. South–South and triangular cooperation should be facilitated, and information, skills and technologies should flow in several directions.

Respect for human rights and fundamental freedoms are international obligations, and are especially relevant because of the expansive potential of both CCB and ICTs. For example, a state delivering CCB should consider whether any skills, resources or technologies they provide might be used in ways that could infringe upon rights and freedoms, such as the monitoring of political dissidents or activists. **Non-discriminatory** CCB should be cognizant of applicable international instruments, such as the UN Convention on the Rights of the Child, the Convention on the Elimination of all Forms of Discrimination Against Women, and the International Convention on the Elimination of All Forms of Racial Discrimination.

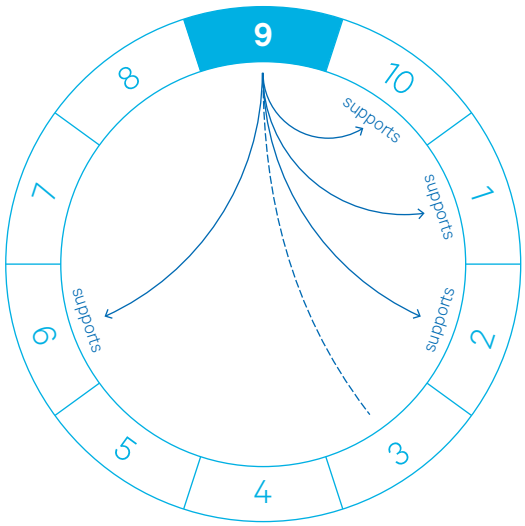
* Emerson-Keeler, E., Swali, A. and Naylor, E. (2023), *Integrating Gender in Cybercrime Capacity-building: A Toolkit*, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135515.

How does this principle help achieve international peace and security?

Human rights and fundamental freedoms are enshrined in law and respecting them strengthens the international order. Furthermore, the UN's women peace and security (WPS) agenda points to the many ways gender mainstreaming can contribute to international peace and security, including in cyberspace.

This principle contributes to international peace and security by ensuring that all states and all actors are treated with respect and held to the same standards.

How does this principle work with other principles?



Principle 9 **supports** Principles 1, 2, 6 and 10. Capacity-building that is gender-sensitive, inclusive and rights-respecting is more likely to lead to sustainable and positive results (Principles 1 and 2). It is also more likely to be conducive to partnerships with mutual trust (Principle 6) and to protecting the confidentiality of sensitive information (Principle 10).

Principle 9 and Principle 3 have a multi-faceted relationship, sometimes complementing each other and sometimes resulting in tension. Capacity-building that adheres to international law and norms is more likely to be politically neutral (Principle 3). At the same time, respect for gender sensitivity, human rights and fundamental freedoms may necessitate articulating conditions around, for example, how resources will be used.

10 The confidentiality of sensitive information should be ensured.

The **confidentiality of sensitive information** is ensured when robust data protection measures are implemented and followed, which adhere to relevant local and international legal frameworks. All parties in the CCB activity should determine what sensitive information is being processed or stored as part of CCB activities and put in place the necessary risk assessments and measures to protect confidentiality. The international nature of CCB may mean that the data protection regulations of several jurisdictions are relevant; as such, actors should work to deconflict responsibilities and ensure the highest possible protection.

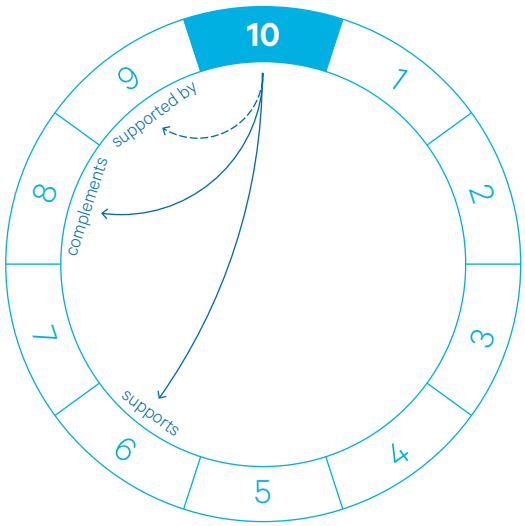
This principle differs from Principle 8 in that it refers to types of information beyond national policies and plans, such as data. Additionally, this principle refrains from placing the responsibility inherent in it on 'all partners', nodding to the greater responsibility on states to safeguard sensitive information. Where CCB relates to large government programmes (e.g. digital ID schemes) or vulnerable groups (e.g. awareness-raising in schools), the importance of protecting sensitive information and personal data is heightened.

Ensuring confidentiality, as opposed to 'respecting' or 'protecting', positions this principle as a foundational principle in CCB delivery, recognizing the adverse effects that data breaches or data mishandling can have on governments, organizations and individuals.

How does this principle help achieve international peace and security?

This principle supports international peace and security by building trust and by protecting CCB as a field of international cooperation from the risk of a major data leak of sensitive information. Such an incident could result in reputational damage for actors involved in CCB, thus damaging the enterprise as a whole.

How does this principle work with other principles?



Principle 10 **supports** Principle 6 by establishing mutual trust and confidence among all parties that the confidentiality of sensitive information related to them, or for which they are responsible, will be ensured.

Principle 10 **complements** Principle 8 as both relate to the confidentiality of information. The urgency of these two principles differs slightly, but they are both complementary, cautioning sensitivity in handling information.

Principle 10 is **supported by** Principle 9 because CCB that respects the right to privacy is more likely to elevate the confidentiality of sensitive information and personal data as a priority.

Section 3. Operationalizing the CCB principles in a project

This section considers three phases in the lifecycle of a CCB project – design, implementation and evaluation – and provides suggestions for how each of the 10 principles might be applied in practice. The suggestions are not an exhaustive list of the ways in which the principles might be applied, and the principles might not be applicable in every project of this type. Rather, they are intended to be an aid that practitioners could use to generate ideas on how to follow a principles-based approach in their own CCB activities and contexts.

An actor's role(s) in CCB – as a donor, implementer, beneficiary or stakeholder – influences what involvement they would have in employing the suggested guidance. However, the suggestions are not organized or grouped by role, as many of the activities will require collaboration between different roles and many actors will play more than one role in a project. Further research can develop suggestions for operationalization specific to each stakeholder group. In any CCB activity, these suggestions should be viewed as guiding rather than prescriptive steps, given the importance of the context of the CCB activity.

The example project in this section is one in which CCB is provided to support a national computer security incident response team (CSIRT) as it creates a national point of contact (NPOC) to join the OEWG POC network and seeks to improve capability for sharing cyberthreat intelligence (CTI).

In the ongoing OEWG discussions, all UN member states agreed on efforts towards establishing a global, inter-governmental points of contact directory (POC). Guided by the principles of sovereignty and non-intervention, the POC network is meant to be a confidence-building measure that aims at enhancing cooperation among states, enabling coordinated responses to ICT incidents, promoting information-sharing, and facilitating secure communication to prevent and

address critical ICT incidents. The POC is meant to complement national computer emergency response teams (CERTs) and CSIRTs networks.[13] Each state is requested to nominate a national point of contact (NPOC) as their representative to the OEWG's global POC directory.

Specifically, in the example project used in this section the following activities are envisaged:

- Training and advice for the NPOC and supporting CSIRT staff on how to engage with, and make best use of, the OEWG's NPOC network.
- Technical assistance to the national CSIRT so that it can install and use a cyberthreat intelligence-sharing (CTI-sharing) platform (e.g. Malware Information Sharing Platform – MISP) that will help it to securely share threat intelligence with other CSIRTs.
- A national exercise to prepare for a scenario in which time-sensitive information is received through the NPOC network or CTI-sharing platform.

For the purpose of this example, the CSIRT is assumed to be within the government and of a level of maturity that is ready to establish an OEWG NPOC role and effectively use a threat intelligence-sharing platform. These niche capabilities were chosen because they are of interest to the OEWG and allow for different aspects of the principles to be explored – it is not a reflection on their priority *vis-à-vis* other capabilities. Additional resources that can assist with the principles are suggested in Annex B.

To generate suggestions for how the principles might be operationalized in the example project, the authors combined insights from the two consultations (see Section 2), with a review of principles implementation toolkits from related fields and reports from capacity-building projects. A conference run by Chatham House in November 2022 – Strengthening Cyber Resilience Conference: Lessons on Cybersecurity Capacity Building from the UK's Digital Access Programme – was also a source of lessons from past CCB projects.

Using the factsheets presented in Section 2 and the above sources, the authors first mapped what the design, implementation and evaluation phases of such a CCB project could look like. Phases were sub-divided into key components to make it easier to describe the different ways in which principles might be operationalized within them. For example, the implementation phase was sub-divided into the work of implementing activities and managing risk on the one hand and monitoring and reporting on the other. This is not a proposed framework for structuring the management of a CCB programme, but rather a framework for exploring and describing the principles' operationalization.

Within the three-phase framework, the authors considered how a principles-based approach might be operationalized throughout the CCB life cycle, applying suggestions from the literature, workshops and conference. The options this

13 United Nations (2023), *Draft Annual Report of the Open-ended working group on security of and in the use of information and communications technologies 2021-2025*, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_27_July_2023.pdf.

generated are presented below to aid CCB practitioners to develop their own ideas for operationalizing the principles in their unique contexts. The guidance in this project example is comprehensive but framed to ensure that all actors involved in the project are able to understand the necessary considerations in the project's design, implementation and monitoring. As such the guidance is not intended to be directed exclusively at one particular actor type.

Figure 3. Implementing the OEWG CCB principles

Phase 1. Design

Gather information and consult	
Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	Conduct a risk and impact assessment that considers the risks to the sustainability of the project's outcomes and any potential risks to the project's longevity.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Consider whether any aspect of the planned project might run counter to the shared objectives and how to mitigate this. The risk assessment for a project with a CSIRT might consider, inter alia, whether any capabilities were being shared or developed that were offensive, dual-use or could be used to disrupt access to the ICT environment. Another important factor to consider is where the CSIRT sits within the government architecture – the context of a CSIRT under an intelligence agency or defence ministry will be different to one under a ministry of ICT.
Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	Conduct a review of the evidence of past lessons and good practices from similar projects. Use relevant good practice guides and studies (many of which are collected on the Cybil Portal) and speak with practitioners and experts in the CSIRT community and POC network organizers through interviews and workshops.
	Use evidence to conduct a baseline assessment of the current CSIRT capacity. Make use of any existing maturity or needs assessments to avoid reinventing the wheel.
	Collect and analyse evidence to understand the context and risks of the project. This may include stakeholder mapping, a political economy analysis and a threat landscape assessment. The latter is especially important to ensure continuity between governments/administrations, and should include a thorough financial assessment
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Ensure that the appropriate state ministries and agencies support the project and that all formal approvals required are in place. It is good practice to have approvals and agreements in writing for accountability and to reduce the risk of misunderstandings later in the project. In this example project the national CSIRT is assumed to be a government body, but its mandate and position within the government structure will nonetheless be a key consideration for how to ensure the correct approvals are in place.
Principle 5 Access to relevant technologies may need to be facilitated.	Assess whether there are any reasons, such as human rights risks, why a technology should not be provided or supported by the project.
Principle 6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.	Establish what the national priorities and plans are for CSIRT development through consultations with the CSIRT, government, experts and stakeholders. Review any published strategy or business plan documents that are relevant.
	Identify the original source of the project idea as that will affect who is likely to feel ownership and how much work is needed to ensure the CSIRT and host country have ownership.
Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	Use stakeholder mapping to help identify potential partners and interested (and affected) parties. This is likely to identify some core parties with a high level of responsibility for success (e.g. the CSIRT, donor and implementer) and parties that could play a useful supporting role, such organizations in the local ecosystem (e.g. sectoral CSIRTS) or the POC network secretariat.

Principle 8 The confidentiality of national policies and plans should be protected and respected by all partners.	The CSIRT could identify which national policies and plans the donor, implementer and other partners need access to and what they might have unintended access to. Applying this principle requires ensuring confidentiality and discretion when using and accessing these national policies and plans, in line with requirements stipulated by the government the policies and plans belong to.
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Conduct a human rights impact assessment of the project activities or outcomes. The training in CTI-sharing protocols and platforms should be considered within the context of the increase in CTI capability. How will the CSIRT collect CTI and will this include accessing people's social media profiles and personal information? How will this information be processed? Who will use the information, including external parties it is shared with, and for what purposes?
	Consult people who will have information about the potential human rights implications of a project (e.g. vulnerable groups, civil society, independent experts) and, where appropriate, involve them in the design.
	Identify the potential impacts of new or enhanced capabilities on different genders and vulnerable groups. Depending upon the project and context, it may be appropriate to conduct a gender impact assessment supported by an inclusion specialist. Adapt to the project scope and local context: some projects have little direct connection to vulnerable groups, while others may, for example, directly bolster a national CSIRT's work supporting the police on child exploitation and online protection.
	Include representatives from diverse gender backgrounds and experts in gender mainstreaming in stakeholder consultations. This representation must be meaningful and stakeholders should be given an opportunity to substantively contribute to the project design and development.
Principle 10 The confidentiality of sensitive information should be ensured.	In this project there may be sensitive information and personal data passing through the intelligence-sharing process. There may also be personal data generated or processed that relates to the CSIRT or project staff, CSIRT customers and stakeholders. The CSIRT could conduct a data privacy impact assessment and a risk assessment covering any other sensitive information the project may handle, with support from the project implementer. This will identify and categorize different types of sensitive information and personal data relevant to the project and determine the level of sensitivity necessary.
	Understand the legal frameworks and data/information protection policies of the jurisdictions in which the project will operate or handle information.
Define the scope and goals	
Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	Identify the sustainable outcomes the project should contribute to. For example, the project may be intended to improve the response to incidents through communication among the POCs. Use a theory of change to work backwards to understand how this will be achieved and the role of the project activities. Include assumptions, for example if you are expecting the POC network organizers to provide training.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Set a clear purpose for the capacity-building by defining what the results should be: what will it look like when the POC and intelligence-sharing are working well once the project is completed? Involve all parties and key stakeholders in goal-setting. In this case, that would include involving the CSIRT, the POC network organizers and any stakeholders in determining how and what CTI is shared.
	Describe the results in a specific, measurable and time-bound way. For example, consider whether timeliness or the quality of the intelligence the CSIRT aims to share can be defined.
	Consider how the results you are aiming to achieve make progress towards the shared objective.

Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	Map the accountability and transparency relationships within the project, including: • the government and citizens of the countries partnering in the capacity-building; • other stakeholders to the project (e.g. the POC network and CSIRT constituencies); • contractual relationships (e.g. if an implementer or trainer was contracted); • members of the international community and other capacity-builders.
	Identify whether there are any other principles that might require mutually agreed conditions. For example, the sustainability of the results (Principle 1) might require that the CSIRT commits to sustaining the POC position and planning for the selection and training of a successor.
	All partners, especially the donor and CSIRT, should discuss how to minimize conditions while ensuring maximum commitment to all relevant principles.
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Design the project so that it aligns with relevant national strategies and plans, respecting how the partner country intends to use the CSIRT function and where they envision it will sit in their national cyber resilience. This may include a national cybersecurity strategy and the CSIRT's mandate and business plan. Partner governments have an important role in this as they are responsible for ensuring that such documents are in place and are respected.
Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	Identify the core parties in the project – including the CSIRT, donor, implementer, etc. – and then agree how a partnership approach will be applied in the project and which other partners could be involved, including from outside government (e.g. the POC network; Forum of Incident Response and Security Teams (FIRST); regional organizations; International Telecommunications Union (ITU); and private sector constituents of the CSIRT).
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Include representatives from diverse gender backgrounds and experts in gender issues in stakeholder consultations to contribute to the project design and training material development.
Technical design and planning	
Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	Take proactive steps to ensure the sustainability of the developed capabilities. During the design phase, identify and assess the necessary resources, anticipate policy adjustments and plan additional activities that will be essential for long-term maintenance. Plan how the necessary resources will be put in place. Secure commitments to sustainability before implementation where possible.
	Make use of open source and low-cost solutions where possible to reduce the future costs of sustaining the capabilities for the CSIRT. The MISP threat-sharing platform is an example of a trusted open-source tool.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Follow a results-based management approach: work backwards from the desired end results to identify the necessary inputs, activities and outputs. Map the logical connections between these, and any assumptions, so that it is clear how you will achieve the results.

Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	All the parties to the project, especially the donor and CSIRT, should agree how best to achieve mutual accountability and transparency. This might be recorded or confirmed in writing for reference.
	Mainstream accountability and transparency into the planning process and steps, for example by preparing a reporting schedule and a stakeholder engagement and communications plan that will provide all partners and stakeholders (e.g. the wider POC network, CSIRT customers and ministry overseeing the CSIRT) with the information they need to monitor the project and hold all involved actors accountable.
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Design the project in compliance with local laws. For example, in a CSIRT support project, legislation would affect what the CSIRT is permitted to do and would influence how it can operate.
Principle 5 Access to relevant technologies may need to be facilitated.	Assess what technologies are required to enable CTI-sharing and establish the POC capability. This may include hardware, software infrastructure for connectivity. Consult with the CSIRT on what they already have or have access to, where there are gaps, and what is affordable within their budgets. In the case of this project, the most important enabling technology would be any information-sharing platform used by the POC network and tools for handling and sharing CTI.
	Consider what barriers there may be to the CSIRT acquiring this technology and how to overcome these.
	Where possible use open-source options for any capabilities that require new software purchases or licensing. An example for this project would be the free MISP threat intelligence-sharing platform.
	When introducing new equipment or software, ensure plans are in place for maintenance, patching, licence renewals and end-of-life replacements. This will ensure that staff are able to continue using it after the project.
Principle 6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.	Design the project around the CSIRT's business plan and objectives for the coming years.
	Describe how the activity aligns to national cybersecurity priorities and plans in project documentation, including any theory of change.
Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	Include all partners and stakeholders in the design of the project.
	Develop stakeholder engagement and communication plans that are inclusive, culturally sensitive and meet the needs of all parties, not just the core ones.
Principle 8 The confidentiality of national policies and plans should be protected and respected by all partners.	The implementer could propose tools and procedures that enable compartmentalization, access controls and auditing for sensitive data flows. It should also ensure its own staff and any subcontractors are familiar with the policies, procedures and tools that will be applied and have the necessary security clearances.
	The implementer could prepare an information/data-sharing agreement for the CSIRT's approval, outlining each partner's responsibilities for protecting confidential information. This could be referenced or included within the project agreement document (e.g. exchange of letters, MoU or contract). Assign roles and responsibilities for implementing the agreement.
	The implementer and CSIRT should agree a notification method and contingency plans for confidentiality breaches, unintended disclosures and loss of sensitive data.

Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Make a plan to mitigate and monitor any human rights risks. For example, the training might cover the legal, ethical and human rights aspects of intelligence-handling and sharing. There might also be organizational safeguards that can be put in place around new capabilities, such as amendments to CSIRT policies and procedures.
	Incorporate good practices on gender sensitivity and inclusivity into the design of the training and its materials. Enable all trainees to participate fully regardless of gender, age, disability, seniority within the organization or other factors that might affect engagement.
	When the project will create or change roles, as this example project will, consider how to prevent discrimination or unconscious bias in staffing and recruitment decisions.
Principle 10 The confidentiality of sensitive information should be ensured.	If necessary, develop an information security policy for the project that outlines how sensitive information will be managed and protected, ensuring compliance with legal and regulatory requirements related to information security and confidentiality.
	Before starting the project, ensure that the respective parties understand their responsibilities and that staff and contractors have the necessary awareness of policies, training and tools to be able to fulfil them.

Other preparatory activities

Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	The government should begin putting in place the necessary resources and plans to sustain the POC and CTI-sharing systems, for example by allocating budgets and updating the national CSIRT's medium- to long-term plans.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	The CSIRT and wider government can prepare the ground for results-focused capacity-building by producing a national cybersecurity strategy and a CSIRT business plan that describes how they want the CSIRT to develop.
Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	The donor should publicize contract opportunities, include clear reporting and communications expectations in the statements of requirements and inform/consult relevant communities (e.g. other capacity-builders) about the upcoming project.
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Secure all necessary approvals before commencing capacity-building to recognize states' authority over their domestic affairs. In the case of the example project, this might be achieved by first consulting the CSIRT, any ministry or agency that oversees it and the ministry responsible for international affairs to identify which approvals will be necessary and from whom.
Principle 6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.	One way to increase ownership by the CSIRT would be to give it responsibility for selecting or contracting the training organization and selecting which intelligence-sharing platform it uses.
Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	To the extent possible, separate the negotiation of partnerships from commercial decisions or grant awards. This helps mitigate power imbalances in partnerships and supports longer-term thinking. For example, in this project the CSIRT may wish to negotiate a long-term training partnership with a tech company separately from its purchase decision on software.

Phase 2. Implement

Implement, manage risk

Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	The host government should commit to future budgetary support for the national POC and intelligence-sharing capabilities. Establish protocols for succession planning to ensure seamless transitions when personnel changes occur.
	Work with trainers who are local or in voluntary peer community networks and consider train-the-trainer approaches, so that there is an enduring capability to provide similar training in the future.
	Find partners whose support can continue after project completion. The NPOC network itself may have resources or benefit from CCB projects that could provide follow-on support to the CSIRT. There are also international organizations dedicated to supporting CSIRTs, such as the FIRST and the ITU, and clearing-house mechanisms that can match needs to capacity-building.
	Prepare and implement a handover and sustainability plan to transfer knowledge and responsibilities that will support continuity beyond the end of the project.
Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	The host government can reduce the risk of politicization by recognizing the importance of the CSIRT's technical expertise and political neutrality. Formal policies and and an empowering informal culture can help separate the CSIRT from the party-political influences that may affect other parts of government.
	Where possible, support and work with local experts and institutions who act as knowledge centres and can help encourage best use and sharing of evidence. For example, the project might work with a local university, cybersecurity training facility or a regional organization like the Asia-Pacific Network Information Centre (APNIC) as a knowledge partner.
	For accountability, have a mechanism by which complaints or concerns about the project can be (anonymously) raised both internally and externally.
	For transparency, have a mechanism by which the public and relevant stakeholders can request information about the project. Many CSIRTs have a website and social media accounts they could use to communicate the project and provide a way for questions to be submitted.
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Deliver the project as it has been agreed with the partner government and stakeholders. Act with transparency so that this can be monitored by all project partners.
	Be careful not to undertake any activities that might be misconstrued as infringing upon state sovereignty. For example, in this project the donor and implementer teams should consider how they engage with the partner team.
Principle 5 Access to relevant technologies may need to be facilitated.	A handover plan at the end of the project should include details on how to sustain the project and the intended use of the technology.

Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	Sustain the active involvement of all parties in the project throughout its delivery, engagement, governance and reporting processes. In practical terms, there may be a regular meeting of core partners to review progress and make decisions, with other parties kept informed through clear communication and consultations ahead of key decisions.
	Some partners may require assistance to participate as partners. For example, the POC network organizer may need assistance visiting the CSIRT and additional information to understand the project and how they can best engage with it.
	The CSIRT itself may need additional support to equitably engage in the governance, design and monitoring of the project. Their staff may be very busy and unfamiliar with the decision-making processes in an international capacity-building project.
	Provide training and awareness-raising so all parties and their staff understand their responsibilities for respecting confidentiality under the agreements in place.
Principle 8 The confidentiality of national policies and plans should be protected and respected by all partners.	Protect the confidentiality of national policies and plans by applying the policies and procedures agreed during the design phase.
	Apply the rule of minimum exposure – only share what is necessary to accomplish the project's objectives.
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Put in place risk mitigation measures and apply any new policies and guidelines. Apply a continuous human rights management approach rather than a one-time risk impact assessment.
	Apply the gender sensitive and inclusive approach that has been designed for the advisory support and training. This may include ensuring training materials are accessible, offering flexible training formats and providing awareness training to the trainers themselves.
Principle 10 The confidentiality of sensitive information should be ensured.	Implement the security controls that were defined in the design phase. These may include technical safeguards such as encryption, access control mechanisms and secure communication channels. They may also include safeguards around physical access to the CSIRT premises and how documents and IT assets are to be protected when off-site.
	Apply an incident response plan in the event of a breach or unauthorized disclosure of sensitive information.
	In this project the design, implementation and monitoring of the security controls can itself be a learning opportunity for CSIRT staff, linked to how they handle sensitive intelligence.
Monitor and report	
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Conduct results-based monitoring to see if the project is meeting the interim targets and adjust the approach if you are off-track.
	Make use of and develop qualitative and quantitative sources of information, such as feedback from the POC network and CSIRT customers, and the data that can come from the CTI-sharing platform.
	Monitor the project's progress to ensure that any changes to the scope or design have not altered its relationship with the shared objectives of an open, secure, stable, accessible and peaceful ICT environment.
	Make the CSIRT central to the process of monitoring and taking decisions on any adjustments. The CSIRT should feel ownership of the process; they hold most of the information needed and they will be most affected by any change of plan and the achievement of a successful result.

Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	Apply an evidence-based monitoring, reporting, evaluation and learning (MREL) process to assess the quality of the evidence used to monitor and evaluate the project.
	All parties should implement their reporting, stakeholder engagement and communications plans. Make use of the POC network itself as it is designed for communicating.
	Monitor the risk that politicization or conditionality might arise during implementation. For example, in a project where new roles are created, consider how the appointment is made and whether it is meritocratic or influenced by political affiliation.
Principle 5 Access to relevant technologies may need to be facilitated.	Monitor how the technology is being used and how risks are being mitigated. Adjust the project plan if needed.
Principle 6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.	Monitor demand for the project and whether the CSIRT is taking ownership of the new role and functions. Indicators might include whether the CSIRT has allocated a budget for the POC and future training, and whether its business plans reflect the new capabilities.
	The reporting and governance structures of the project should reflect local ownership. The CSIRT should be actively involved in guiding the project, receiving reports and asking questions.
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Include human rights indicators in monitoring and evaluation.
	Where possible, use indicators in the monitoring and evaluation process that will enable assessing the effectiveness of the training across different groups.

Phase 3. Evaluate

Evaluate	
Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	Evaluate the longer-term, sustained impact of the project. For example, follow up three years later to see if the CSIRT is still an active member of the POC network and how CTI is being shared.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Evaluate whether the defined and measurable results of the project were achieved. Evaluate the contribution the project made to the shared objectives.
	Engage local experts in the monitoring and evaluation to strengthen local capacity and ensure culturally relevant assessments.
Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	Apply an evidence-based approach to evaluation. Make use of quantitative and qualitative data. Involve subject matter experts who can challenge the approach and advise on the strength of the evidence being used. Consider using independent experts to conduct the evaluation in an impartial manner.
	In the evaluation, consider how well the designed approach to accountability and transparency was implemented.
Principle 4 Capacity-building should be undertaken with full respect for the principle of State sovereignty.	Evaluate whether any state sovereignty issues arose during the project and whether any lessons for applying this principle can be learnt.
Principle 6 Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.	Support national ownership by conducting the evaluation with the CSIRT and not of the CSIRT. If there is strong ownership, the CSIRT should be interested in the findings and keen to include evidence of success in its internal reporting.
Principle 7 As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.	Engage all partners in the evaluation process. Solicit feedback from stakeholders. Use the evaluation to learn lessons that will make the longer-term partnerships stronger and celebrate success.
Principle 8 The confidentiality of national policies and plans should be protected and respected by all partners.	The project should assess whether there were any breaches of confidentiality or weaknesses identified in the safeguards put in place. Learn lessons for improving confidentiality protections in future partnerships and capacity-building activities.
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Assess performance against human rights indicators in the monitoring and evaluation (M&E) framework. Revisit the training and CTI-handling after the project has been completed to see if the relevant good practices, procedures and policies implemented during the project have been sustained.
	Analyse the gender disaggregated data that was collected during the monitoring and conduct additional interviews to assess the effectiveness of the gender sensitive and inclusive approach.

Principle 10 The confidentiality of sensitive information should be ensured.	Assess the success of the security measures to learn lessons and inform future projects and CSIRT procedures.
Identify and share lessons and knowledge	
Principle 1 Capacity-building should be a sustainable process, comprising specific activities by and for different actors.	Identify and share lessons from the project that could improve sustainability in future capacity-building.
Principle 2 Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.	Identify and share lessons, for example through the POC network and CSIRT communities such as the FIRST.
Principle 3 Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.	Contribute back to the pool of evidence for capacity-building, for example, through sharing lessons learnt with the POC network or by publishing a blog on the data sources used to measure whether the CSIRT was sharing more and better intelligence after the project.
	Publish the programme evaluation so that others can make use of it as evidence. This should be agreed with the CSIRT and they should be involved in making any redactions of sensitive information.
Principle 5 Access to relevant technologies may need to be facilitated.	Review lessons around facilitating technology access, including the suitability of solutions to the local context and sustainability of access after the project. As the project supports essential CSIRT functions, there is considerable potential to share lessons with the CSIRT community and its capacity-builders.
Principle 9 Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.	Integrating human rights and fundamental freedoms, gender mainstreaming and inclusive practices into capacity-building can be difficult, especially to partners who do not see or understand the value and benefit of such an approach. Learning and sharing lessons on how to respect rights and freedoms, and be gender sensitive and inclusive, adds to the global CCB ecosystem positively and constructively by contributing an evidence base on how to design, implement and re-evaluate rights-respecting CCB projects. This can be done in written documentation or through seminars or workshops, essentially becoming a form of capacity-building itself.

Source: compiled by authors.

Conclusion: Sustaining momentum for a principles-based approach to CCB

In the rapidly evolving cyberspace landscape, where technological advancements present both opportunities and challenges, CCB has emerged as a top priority. This is due to the role of CCB both in helping states safeguard their critical infrastructure against cyberthreats and in ensuring ICTs enable states to achieve prosperity and economic development. In recent years, efforts have been dedicated to maximizing the effectiveness of CCB activities and ensuring that they are conducted in a responsible way. This process has mainly focused on developing and advocating for a principles-based approach to CCB, particularly through the adoption of the OEWG CCB principles.

As this paper has explored, there is not one way of following a principles-based approach to CCB. The principles can – and should – be interpreted and applied to suit particular contexts. However, the significance, benefits and utility of a principles-based approach is clear: the standardizing function of the principles in CCB activities can help to make CCB more efficient and effective, supporting responsible delivery and contributing to the objective of an open, secure, stable, accessible and peaceful cyberspace, while encouraging a broader adherence to the UN framework of responsible state behaviour in cyberspace.

A clear understanding of the principles, as well as their context and implementation, is imperative for an effective principles-based approach to CCB. In Section 1, this paper highlighted the critical role CCB plays in empowering states to leverage ICTs for economic development and security, and the potential of CCB principles to prevent misuse, and ensure effective and equitable implementation.

In Section 2, this paper considered the principles themselves, looking at what they entail, how they play their part in a secure cyberspace and their relationship with other principles. In Section 3, this paper provided actionable and practical guidance on how to implement the principles.

From this exercise and analysis, two specific conclusions become apparent. First, the CCB principles encompass and contribute to a variety of objectives, from those elaborated within the OEWG to broader SDGs. Their purpose is not limited to contributing to the objectives outlined in this paper, and the technology-neutral drafting of the principles guarantees their broader and continued relevance. This is important because it ensures that the CCB principles remain flexible and adaptable for a cyber landscape that is rapidly developing. It is also an implicit recognition of the fact that CCB is not a static endeavour: as development and technology needs evolve, so will CCB, and both CCB and international development will need to align. Thus, as states continue their deliberations at the international level, within the current OEWG and elsewhere, it is important for them to identify connections to other fields and make greater efforts to share experiences and lessons learned. This can ensure that CCB is not isolated from international development and that a principles-based approach to CCB can draw on decades-long experience and practice.

Second, embracing a principles-based approach to CCB activities necessitates proactive engagement from the CCB community at various levels. Despite being developed in a state-led forum and existing within a framework that outlines responsible *state* behaviour in cyberspace, the principles are clear that CCB requires broader buy-in and is not exclusively a state responsibility. To this end, efforts at the international and regional levels should focus on raising and sustaining awareness of the OEWG principles, facilitating the sharing of experiences, building connections with related principles and actively engaging a diverse range of stakeholders. This broader involvement of the CCB community should be facilitated creatively and regularly, respecting the modalities of the current OEWG while recognizing its limitations. Recent OEWG initiatives to elevate the importance of CCB – such as the Global Roundtable on ICT Security Capacity Building held in May 2024 – can offer an important forum to discuss and promote the principles further.[14]

At the national level, states should prioritize integrating these CCB principles into their national processes, policies and training frameworks, and formally declare their intentions to apply the principles to promote transparency and inspire others. States should also support initiatives led by the CCB community that are focused on operationalizing the principles. Multi-stakeholders, including governments, civil society, academia and the private sector, should voluntarily align their practices with the OEWG principles and integrate them into their organizational frameworks, supporting the implementation through awareness-raising, developing resources, conducting research and providing training.

14 Permanent Mission of the Republic of Singapore (2024), 'Letter from OEWG Chair to Stakeholders on Global Roundtable', United Nations Office of Disarmament Affairs, 27 February 2024, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_to_Stakeholders_on_Global_Roundtable_27_February_2024.pdf.

Such a comprehensive and inclusive approach will ensure that CCB activities are not only effective, efficient and equitable but that they contribute to the ultimate objective of an open, safe, secure, accessible and peaceful cyberspace. By engaging all relevant actors and promoting broader adherence to responsible state behaviour in cyberspace, CCB can significantly enhance global cyber resilience and security.

About the authors

Joyce Hakmeh is the deputy director of the International Security programme at Chatham House and co-editor of the *Journal of Cyber Policy*. She specializes in cyber policy, including cybersecurity, cybercrime and cyber governance, and provides regular analysis on issues that sit at the nexus between technology and geopolitics.

In addition to her regular research and writing, Joyce's current work includes leading civil society engagement in UN processes on cyber issues, delivering immersive simulation exercises, building cyber capacity and expertise among policymakers, facilitating dialogues and developing strategic approaches to tackling cybercrime and addressing equality, diversity and inclusion in cyber policymaking.

Amrit Swali is a research associate in the International Security Programme and on the editorial team for the *Journal of Cyber Policy*. Amrit works on projects focusing on cyber governance, cyber capacity-building, equality, diversity and inclusion (EDI) in cyberspace and technology, and cybercrime. Amrit is also co-chair for gender on Chatham House's EDI Working Group.

Amrit holds an MSc in the history of international relations from the London School of Economics and Political Science, and a BA (Hons) in history from the University of Southampton.

Robert Collett is an adviser, writer and speaker on international cybersecurity capacity-building. From 2019 to 2020, he was the UK's first seconded senior adviser to the Global Forum of Cyber Expertise (GFCE). Prior to this he ran and expanded the UK's international cybersecurity capacity-building programmes.

Robert has a 17-year track record leading programmes and policy initiatives as a UK diplomat, working at the intersection of foreign policy, security and development. During this period, he gave evidence to a Lords committee, led the strategic communications for NATO's Provincial Reconstruction Team in Helmand and managed a series of challenging projects from de-mining to countering violent extremism and cybersecurity.

Acknowledgments

We are grateful for the support of the Ministry of Foreign Affairs of the Kingdom of the Netherlands for enabling this project and for their support and guidance throughout its delivery. We thank the project's advisory group, the anonymous peer reviewers and the International Security Programme at Chatham House for their feedback on this output's approach and substance. We are particularly grateful to the many OEWG stakeholders who attended consultations or provided insights that directly contributed to this output. We also thank Mike Tsang in the Communications and Publishing Department at Chatham House.

Annex A. Principles frameworks relevant to CCB

Framework	Details
Principles of effective development cooperation[15]	These principles apply to any CCB that can be classified as international development and especially any activity using Overseas Development Assistance funding. They were agreed in 2011 by 161 countries and 56 organizations. The four principles are: country ownership; focus on results; inclusive partnerships; and transparency and mutual accountability.
Global Forum on Cyber Expertise (GFCE) principles for CCB[16]	The GFCE agreed a set of four principles for CCB in its 2017 Delhi Communique that were explicitly inspired by the effective development cooperation principles. The GFCE's principles are: national ownership; sustainability; inclusive partnerships and shared responsibility; and trust, transparency and accountability.
Principles for Digital Development[17]	The Principles for Digital Development were created in 2014 and updated in 2024 under the stewardship of the United Nations Foundation's Digital Impact Alliance. Over 250 organizations have now endorsed the nine principles: design with the user; understand the existing ecosystem; design for scale; build for sustainability; be data-driven; use open standards, open source and open innovation; reuse and improve; address privacy and security; and be collaborative.
Principles on Identification for Sustainable Development[18]	The World Bank first published 10 Principles on Identification for Sustainable Development in 2017 and refreshed them in 2021. They are grouped under three pillars: inclusion (universal coverage and accessibility); design (robust, secure, responsive and sustainable); and governance (building trust by protecting privacy and user rights).
Donor Principles for Human Rights in the Digital Age[19]	The Freedom Online Coalition of 38 governments published their Donor Principles for Human Rights in the Digital Age in 2023. The nine principles cover: aligning laws and regulations with HR; strengthening democratic digital governance; partnering with the private sector for rights-respecting investment; HR impact assessments; prioritizing digital inclusion; fostering alliances; growing a rights-respecting technology workforce; ensuring digital security and safety; and promoting the principles.

15 OECD (2011), 'Busan Partnership Outcome Document', https://www.effectivecooperation.org/content/busan-partnership-outcome-document.
16 GFCE (2017), 'Delhi Communiqué', https://thegfce.org/tools/delhi-communique.
17 Principles for Digital Development (2024), 'Principles for Digital Development', https://digitalprinciples.org/principles.
18 World Bank (2017), 'Principles on Identification for Sustainable Development: Toward the Digital Age', https://www.idprinciples.org.
19 Freedom Online Coalition (2023), 'Donor Principles for Human Rights in the Digital Age', https://freedomonlinecoalition.com/donor-principles-for-human-rights-in-the-digital-age.

Annex B. Resources for applying CCB principles

Resource	What it can assist with
Results focused	
Operational Guidance: The EU's International Cooperation on Cyber Capacity Building[20] Operational Guidance for the EU's International Cooperation on Cyber Capacity Building[21]	The EU's operational guidance describes a process and contains recommendations for managing results-focused CCB. The first edition also includes example indicators and metrics for results frameworks related to different cyber capacities. The guidance is written for an EU audience, but most of the content is universally applicable.
Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence[22]	This guide provides advice for using and integrating statistics within the day-to-day operations of the criminal justice authorities, but it is also useful for cyber capacity-builders wanting to find and use evidence related to cybercrime.
Results and Indicators for Development: Cybersecurity[23]	This European Commission guidance note contains clear and measurable results statements that are in line with the UN SDGs, along with a range of indicators to monitor progress.
Global Overview of Existing National Cyber Capacity Assessment Tools [24]	Several assessment tools have been developed to (self) assess a country's cyber capacity. This global overview of assessment tools (GOAT) guide helps countries and capacity-builders to see which tools exist, compare their features and access them.
The Art of Knowledge Exchange: A Results-Focused Planning Guide for Development Practitioners[25]	Much of CCB involves exchanging knowledge between officials and experts in different countries. This World Bank guide provides results-focused advice for designing and managing such activities.
Handbook on Planning, Monitoring and Evaluating for Development Results[26]	Although framed around international development and over a decade old, this UNDP handbook contains a lot of practical advice on planning for results-focused capacity-building that can be applied in CCB.
Evidence-based	
Applying Evaluation Criteria Thoughtfully[27]	This is an OECD guide to applying six criteria for good evaluations – relevance, coherence, effectiveness, efficiency, impact and sustainability – that are applicable to CCB.

20 European Commission (2018), *Operational guidance for the EU's international cooperation on cyber capacity building: A Playbook*, https://www.iss.europa.eu/sites/default/files/Operational%20Guidance%20for%20the%20EU%E2%80%99s%20international%20cooperation%20on%20cyber%20capacity%20building%20%E2%80%93%20A%20Playbook.pdf.
21 EU CyberNet, project of the Service for Foreign Policy Instruments, European Commission (2023), *Operational Guidance: The EU's International Cooperation on Cyber Capacity Building*, https://www.eucybernet.eu/operational-guidance.
22 EU, Council of Europe and INTERPOL (2020), *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence*, https://www.interpol.int/content/download/15731/file/Guide%20for%20Criminal%20Justice%20Statistics%20on%20Cybercrime%20and%20Electronic%20Evidence.pdf.
23 European Commission (2018), *Results and Indicators for Development: Cybersecurity*, https://europa.eu/capacity4dev/system/files/documents/sector/sectorpresentation41.pdf.
24 Weisser Harris, C. et al. (2021), *Global Overview of Existing National Cyber Capacity Assessment Tools*, Global Forum on Cyber Expertise, https://cybilportal.org/wp-content/uploads/2021/07/Global-Overview-of-Assessment-Tools_CLEAN_07July.pdf.
25 World Bank (2015), *The Art of Knowledge Exchange: A Results-Focused Planning Guide for Development Practitioners*, Second Edition Updated, http://hdl.handle.net/10986/17540.
26 UNDP (2009), *Handbook on planning, monitoring and evaluating for development results*, http://web.undp.org/evaluation/handbook/documents/english/pme-handbook.pdf.
27 OECD (2021), *Applying Evaluation Criteria Thoughtfully*, https://doi.org/10.1787/543e84ed-en.

Resource	What it can assist with
Development Research in Practice: The DIME Analytics Data Handbook[28]	Written by the Development Impact Evaluation (DIME) team at the World Bank, this guide to using data for research and evaluation in development has methods that can be applied in CCB.
Assessing the Strength of Evidence[29]	This guide provides a method that helps assess the strength of evidence in individual reports or papers as well as make a judgment on the overall strength of evidence in the area of CCB being researched.
How to Do a Rigorous, Evidence-focused Literature Review in International Development: A Guidance Note[30]	Before starting a large programme or intervention, states may wish to review the relevant literature to see what evidence there is, what different types of intervention work and learn lessons from what has been tried before. This guide contains advice that can assist in that process.
Sustainable	
Guide for Developing Sustainability and Transition Plans – V2.0[31]	This guide for USAID is framed around international development healthcare programmes but has best practice advice that is directly applicable to CCB.
Demand-driven and locally owned	
A Demand-Driven Approach to Development: A CSIS Primer[32]	A primer explaining what a demand-driven approach means, why it matters and how it might be implemented.
Accountability	
Frameworks for Mutual Accountability and Enhanced Policy Dialogue [33]	This K4D report, commissioned by the UK's former Department for International Development, provides advice on what mutual accountability frameworks are and good practices for establishing them.
Mutual Accountability: A Guidance Note for National Policy-makers and Practitioners[34]	This guidance note commissioned by the UN Economic and Social Council provides advice on applying mutual accountability that has useful lessons for CCB.

28 Bjärkefur, K. et al. (2021), *Development Research in Practice: The DIME Analytics Data Handbook*, World Bank, https://doi.org/10.1596/978-1-4648-1694-9.
29 UK Department for International Development (2014), *Assessing the Strength of Evidence*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/291982/HTN-strength-evidence-march2014.pdf.
30 Hagen-Zanker, J. and Mallett, R. (2013), *How to do a rigorous, evidence-focused literature review in international development: a guidance note*, ODI, https://odi.org/en/publications/how-to-do-a-rigorous-evidence-focused-literature-review-in-international-development-a-guidance-note.
31 University Research Co (2019), *Guide for Developing Sustainability and Transition Plans – V2.0*, USAID, https://www.urc-chs.com/wp-content/uploads/urc-assist-sustainability-transition-guide.pdf.
32 Bandura, R. and Hammond, M. (2019), *A Demand-Driven Approach to Development: A CSIS Primer*, Center for Strategic & International Studies, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190515_BanduraHammondRunde_DemandDriven_WEB.pdf.
33 Birch, I. (2020), *Frameworks for mutual accountability and enhanced policy dialogue*, K4D, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15587/869_Mutual%20accountability%20frameworks.pdf?sequence=1&isAllowed=y.
34 Bester, A. (2014), *Mutual Accountability: A Guidance Note for national policy-makers and practitioners*, https://www.un.org/en/ecosoc/newfunct/pdf14/ma_guidance_note.pdf.

Resource	What it can assist with
Transparency	
Open Data, Transparency and Accountability: Topic Guide[35]	This DFID-commissioned guide provides general advice on open data, transparency and accountability that is applicable in the CCB context.
Sharing What Matters: Foundation Transparency[36]	This Centre for Effective Philanthropy guide has advice for foundations but will also be of interest to recipients of philanthropic grants and has some lessons for donors.
International Open Data Charter[37]	Open-data good practices help organizations to apply transparency and accountability as well as contributing to better collaboration, research and the development of new CCB tools. The Open Data Charter contains six principles for open data that aim to guide governments in collecting, sharing and using well-governed data in order to respond effectively and accountably to global challenges. Further information and advice are available at https://opendatacharter.net.
When Does Transparency Improve Institutional Performance?[38]	This study examined 20,000 projects in 83 countries to learn when transparency improves institutional performance. It identifies that having and following access to information policies is key.
Human rights-based approach	
Operational Human Rights Guidance for EU External Cooperation Actions Addressing Terrorism, Organised Crime and Cybersecurity[39]	The EU's human rights guidance for its international CCB can provide ideas on how to assess and mitigate human rights risks.
UNDP Digital Standards – Do No Harm[40]	The 'do no harm' digital standard contains useful practices for all capacity-building that is developing or contributing to digital products and services.
The Human Rights Based Approach to Development Cooperation Towards a Common Understanding Among UN Agencies[41]	This short guidance note for UN agencies is useful for organizations working through how to create a framework for applying a human-rights based approach in their own work. The human rights field has progressed in the two decades since it was written, but it may be useful for understanding how the UN originally worked through the same issues.

35 Carolan, L. (2016), *Open data, transparency and accountability: Topic guide*, GSDRC, https://assets.publishing.service.gov.uk/media/5857fdcb40f0b60e4a0000d6/OpenDataTA_GSDRC.pdf.
36 Buteau, E. et al. (2016), *Sharing What Matters: Foundation Transparency*, The Center for Effective Philanthropy, https://cep.org/wp-content/uploads/2019/08/CEP_Sharing-What-Matters-Foundation-Transparency_2016.pdf.
37 Open Data Charter (2015), *International Open Data Charter*, https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf.
38 Honig, D., Lall, R. and Parks, B. C. (2022) 'When Does Transparency Improve Institutional Performance? Evidence from 20,000 Projects in 183 Countries', *American Journal of Political Science,* 67(4), pp. 1096–1116, https://doi.org/10.1111/ajps.12698.
39 Nicole, S. and Hansen, A. (2015), *Operational Human Rights Guidance for EU external cooperation actions addressing Terrorism, Organised Crime and Cybersecurity*, European Commission, https://international-partnerships.ec.europa.eu/system/files/2019-09/manual-hr-guidance-ct-oc-cyber-november-2015_en.pdf.
40 United Nations Development Programme (2022), '5. Do No Harm', UNDP Digital Standards, https://www.undp.org/digital/standards/5-do-no-harm.
41 UNSDG Human Rights Working Group (2003), *The Human Rights Based Approach to Development Cooperation Towards a Common Understanding Among UN Agencies*, https://unsdg.un.org/resources/human-rights-based-approach-development-cooperation-towards-common-understanding-among-un.

Resource	What it can assist with
Gender and inclusion	
A Framework for Developing Gender-Responsive Cybersecurity Policy: Assessment Tool[42]	This assessment tool seeks to provide step-by-step advice and concrete recommendations for those wishing to develop a gender approach to cybersecurity policy.
Manual on Online Gender Violence and its Impact on the Lives of Women and Girls[43]	Information, tools and strategies for countering online gender-based violence. The manual can be used by capacity-builders to better understand the phenomenon of online gender violence, how it manifests and what some response strategies are.
Integrating Gender in Cybercrime Capacity-building Toolkit[44]	This toolkit has been designed for practitioners working to integrate gender considerations in anti-cybercrime capacity-building activities but has insights that are applicable to all CCB. Using a set of example projects, it offers clear steps to promote the gender-sensitive design and implementation of a wide range of capacity-building activities.
Confidentiality of sensitive information	
Handbook on Data Protection in Humanitarian Action[45]	This International Committee of the Red Cross (ICRC) handbook was written for humanitarian organizations but has advice that is applicable in CCB programmes including: basic principles of data protection; legal bases for personal data processing; international data-sharing; data protection impact assessments; and relevant scenario-specific advice such as cloud services and digital ID.
(Multi-stakeholder) partnerships	
The SDG Partnership Guidebook: A Practical Guide to Building High Impact Multi-stakeholder Partnerships for the Sustainable Development Goals[46]	This guide by The Partnering Initiative and United Nations Department of Economic and Social Affairs is framed around building country-level partnerships to achieve the SDGs. It is accompanied by a Fit For Partnering framework and assessment process to help organizations prepare for and improve their partnerships.[47]
Framework for Multistakeholder Cyber Policy Development[48]	This guide by Global Partners Digital provides advice for creating and evaluating multi-stakeholder processes for national cyber policy development that can also be applied to taking a multi-stakeholder approach to capacity-building.

42 Association for Progressive Communications (2023), *A Framework for Developing Gender-Responsive Cybersecurity Policy: Assessment Tool*, https://www.apc.org/sites/default/files/apcgendercyber-assessmenttool.pdf.
43 Morales, K. N. V. (2021), *Online gender-based violence against women and girls: Guide of basic concepts, digital security tools and response strategies*, https://www.oas.org/en/sms/cicte/docs/Manual-Online-gender-based-violence-against-women-and-girls.pdf.
44 Emerson-Keeler, R., Swali, A. and Naylor, E. (2023), *Integrating gender in cybercrime capacity-building: a toolkit,* London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135515.
45 Kuner, C. and Marelli, M. (eds) (2020), *Handbook on Data Protection in Humanitarian Action*, second edition, ICRC, https://www.icrc.org/en/data-protection-humanitarian-action-handbook.
46 Stibbe, D. and Prescott, D. (2022), *The SDG Partnership Guidebook: A practical guide to building high impact multi-stakeholder partnerships for the Sustainable Development Goals,* The Partnering Initiative, https://thepartneringinitiative.org/publications/toolbook-series/the-sdg-partnerships-guidebook.
47 The Partnering Initiative (undated), 'Fit for Partnering', https://thepartneringinitiative.org/training-and-services/supporting-organisations/fit-for-partnering.
48 Kaspar, L. and Shears, M. (2018), *Framework for Multistakeholder Cyber Policy Development*, Global Partners Digital, https://www.gp-digital.org/wp-content/uploads/2018/03/framework_cyberpolicy.pdf.

Cover image: A board used to represent elements of infrastructure of the fictitious country being targeted during the Locked Shields NATO exercise in Tallinn, Estonia, 23 April 2024.
Photo credit: Copyright © Peter Kollanyi/Bloomberg via Getty Images

ISBN 978 1 78413 613 0
DOI 10.55317/9781784136130

Cite this paper: Hakmeh, J., Swali, A. and Collett, R. (2024), *A principles-based approach to cyber capacity-building (CCB): Understanding and operationalizing the OEWG CCB principles*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136130.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

Ministry of Foreign Affairs

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223