How can the cybercrime convention adopt a strategic approach to cybercrime capacity building and protect against potential harms and misuses?

Cyber Policy Team, Chatham House[1]

Introduction

Cybercrime capacity building is an umbrella term used to describe activities that are designed to strengthen the "skills, instincts, abilities, processes and resources that organizations, governments and communities need" to build and sustain strong anti-cybercrime measures.[2] In the context of the ad hoc committee to elaborate a comprehensive convention on countering the use of information and communications technologies for criminal purposes (hereafter, AHC), cybercrime capacity building has gained traction as a key tenet to levelling the playing field amongst Member States, to ensure they all have the appropriate ability and capabilities to counter cybercrime and implement the convention in its fullest, and to ensure smooth and compatible international cooperation on cybercrime investigations.

Generally, it is understood that 'technical assistance' falls under the broader umbrella of capacity building. In previous AHC sessions, Member States have discussed the merits of each term, both in general and in relation to the purpose of this convention. During the third session of the AHC, in response to a question from the Chair, most Member States expressed a preference for using the term 'technical assistance', citing several reasons, including (but not limited to): technical assistance is more specific and targeted than capacity building; technical assistance is inclusive of capacity building activities; and technical assistance is the term used in UNTOC and UNCAC so would be the preferred term in this convention for reasons of consistency. It was largely accepted that, while the two terms are related, they are different.

Chapter V of the convention is dedicated to 'technical assistance, including information exchange', following the model of UNTOC (which contains a chapter on 'training and technical assistance') and UNCAC (which contains a chapter on technical assistance and information exchange').[3] In contrast, other cybercrime specific conventions such as the Budapest Convention

---

[1] This briefing paper is submitted to the fifth session of the ad hoc committee to elaborate a comprehensive convention on countering the use of ICTs for criminal purposes and is part of a multi-year project funded by Global Affairs Canada.

[2] This definition is derived from the United Nation's definition of 'capacity-building': 'Capacity building', www.un.org, <https://www.un.org/en/academic-impact/capacity-building>, [accessed 24 March 2023].

[3] 'United Nations Convention Against Transnational Organized Crime And The Protocols Thereto', United Nations Office on Drugs and Crime, (Vienna, 2004), <https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_T

and the Malabo Convention do not contain specific chapters on technical assistance or capacity building; instead, for example, the Council of Europe's technical assistance and capacity building efforts are coordinated outside of the Budapest Convention, primarily through its Global Action on Cybercrime Extended or GLACY+[4]. The inclusion of a specific chapter on 'technical assistance, including information exchange' in the proposed convention, then, is a clear indication of its importance to the convention's effective implementation, and Member States' priorities and aims. This briefing paper opts for the term 'capacity building' rather than 'technical assistance'. This is because, while there is a specific chapter on 'technical assistance', other areas in the convention go beyond technical assistance and are more appropriately described under capacity building, such as Article 86(1)(c) which goes beyond the technical aspects and addresses the need for a comprehensive approach to countering cybercrime that also includes the human, organizational, governmental and legal elements. Additionally, capacity building or technical assistance conducted under the AHC is not done in a vacuum: other international processes, such as the UN open-ended working group on developments in the field of information and telecommunications in the context of international security (hereafter, OEWG), also cover cyber capacity building.[5] As this paper will argue, enabling linkages between separate avenues of work on cyberspace is not only an efficient practice, but also a practice that will strengthen the convention itself. There are already principles on capacity building that emanated from the OEWG that the AHC can use to strengthen its own capacity building work and that can ensure that Member States are not renegotiating issues that there is already consensus on.

This paper is divided into three sections. Section 1 addresses the intended and unintended harms that can result from cybercrime capacity building efforts, making the case for a human-centric approach in the convention. Section 2 looks at the cybercrime capacity building principles included in Article 86 of the CND and compares them to other existing principles, such as the ones included in the 2021 OEWG consensus report. Finally, Section 3 looks at Article 86(1)(c) of the CND and recommends ways in which it can be made more comprehensive to address all stages of the cybercrime response lifecycle.

Section 1: How can the convention protect against abuse of cybercrime capacity building?

If implemented in a manner that does not respect human rights and fundamental freedoms, cyber capacity building efforts, including cybercrime capacity building, can be exploited and abused, resulting in harms. These harms can be conscious or unconscious, intended or unintended, and can have wide-ranging consequences that impact local communities and state relations. There are several areas for potential harms, misuses and abuses of cybercrime capacity building, but this paper will focus on three.

HE_PROTOCOLS_THERETO.pdf>; 'United Nations Convention Against Corruption', United Nations Office on Drugs and Crime, (Vienna, 2004), <https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf>.

[4] Global Action on Cybercrime Extended (GLACY)+ - Cybercrime (coe.int)

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

Misuse: Tools and skills gained through cybercrime capacity building can be <u>intentionally</u> used for oppressive activities, thus violating human rights and fundamental freedoms.

Often, capacity building activities can include the transfer of tools and skills that are dual-use. This means that they can be used for a variety of purposes, including with malicious intent. Any technical assistance or capacity building activity that is done without a prior human rights risk assessment could contribute to the abuse or misuse of said technical assistance or capacity building.

The CND has recognised this, especially regarding surveillance technologies. Surveillance technologies and capabilities have a legitimate law enforcement use, and are therefore an important aspect of cybercrime investigations and are included in technical assistance and capacity building efforts. Article 87 of the CND lists 'modern law enforcement equipment and techniques and the use thereof, including electronic surveillance, controlled deliveries and undercover operations' as one of the areas that technical assistance programmes might consider.[6]

However, surveillance technologies are particularly prone to abuse and misuse, posing substantial risks to human rights and fundamental freedoms. They disproportionately affect women and girls, who are particularly vulnerable to becoming victim to the hacking of accounts and devices and the use of spyware and surveillance technologies, not just in cases of domestic violence and abuse.[7] They could also be used to disproportionately target certain vulnerable groups, such as marginalized communities or political dissidents. The CND recognises this risk: Article 78 calls for the 'appropriate use by its competent authorities' of forms of surveillance.[8] The transfer of these technologies under the guise of capacity building or technical assistance must come with safeguards that explicitly recognise how said technologies may be put to malicious uses that would violate pre-existing international agreements.[9]

Conditions to capacity building can be an important safeguard to protect against the malign uses of these tools and/or skills. The convention should make explicit reference to these conditions which should be built around the protection of human rights and fundamental freedoms, including those related to gender and other protected characteristics.

---

[6] 'Article 87: Training and technical assistance', *Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of*
information and communications technologies for criminal purposes (CND), United Nations Office on Drugs and Crime, (Vienna, 2023), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/188/31/PDF/V2218831.pdf?OpenElement>.

[7] C. Parsons et al, '"The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry", Citizen Lab, 2019, <https://citizenlab.ca/2019/06/the-predator-in-your-pocket-a-multidisciplinary-assessment-of-the-stalkerware-application-industry/>.

[8] Article 78: Special investigative techniques', *CND,* United Nations Office on Drugs and Crime, (Vienna, 2023), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/188/31/PDF/V2218831.pdf?OpenElement>.

[9] For an example on how the transfer of surveillance technologies under technical assistance or capacity building activities can contribute to harms and be abused, see: https://www.accessnow.org/wp-content/uploads/2021/10/21.10.08_EU_Ombudsman_Complaint_Final.pdf.

Harm: Tools and skills gained through cybercrime capacity building can <u>unintentionally</u> expose people to new vulnerabilities.

This harm is similar to the first but occurs unintentionally, primarily as a result of the provision of tools and techniques through cybercrime capacity building efforts without the necessary level of training and ongoing assurance. This may result in mistakes being made by those who receive the tools and techniques (typically law enforcement officers), causing harm to citizens. Tools that are used to filter black-listed domains (such as domains used for malware command and control) may unintentionally restrict access to legitimate information online. Another example is tools that are aimed at identifying and geolocating criminals' IP addresses; these tools may result in the wrong people being arrested if the investigators are not properly trained.

This problem sits within a larger issue which can be better understood as 'digitization without cybersecurity'. If not coupled with cybersecurity, digitization efforts – which can be conducted through capacity building – can be counterproductive to the aims of the proposed convention, exposing countries and communities to risks otherwise unencountered. Such digitization efforts must be done with inclusion and development principles in mind; different communities and different groups of people will have different requirements that must be understood and met.

Harm and misuse: Cybercrime capacity building can reinforce dangerous or harmful international (political) power dynamics at the expense of equitable transfer of skills, expertise and knowledge.

Often, there are very clear distinctions between which Member States are known as 'donor' countries for cyber capacity building and which Member States are known as 'recipient' countries. These titles and categories fail to consider that technical assistance and capacity building should be reciprocal exercises where each country contributes what it can to a constructive and productive dialogue aimed at improving anti-cybercrime measures for all countries involved, particularly in dealing with this transnational challenge, and has the capabilities necessary to fulfil their part.

Cybercrime capacity building can perpetuate a 'Global North' standard on effectiveness and adequacy when it comes to anti-crime measures. This in turn can negatively impact a holistic and realistic understanding of a country's needs when it comes to capacity building. This 'Global North' standard also limits the space and opportunity for 'South-to-South' cooperation and knowledge-sharing. This idea is further explored in Section 2.

Capacity building, like international development, is thought of and often implemented as a soft power tool. In a geopolitically tense world, there are increasingly expectations tied to funding technical assistance and capacity building. The tendency to conceive of capacity building as a soft-power tool and, subsequently, withholding or limiting such assistance because it does not, for example, further a particular geopolitical aim, is not within the spirit of the AHC nor in line with a principles-based approach to capacity building. Where possible, Member States should consider capacity building requests through a rights-centric lens. Not doing so risks reinforcing dangerous or harmful (political) power dynamics at the expense of the equitable and necessary transfer of skills, expertise and knowledge.

Consideration also needs to be given to how capacity building activities might exacerbate internal power imbalances, for example by transferring capabilities from locally accountable police forces to centralised entities, or by introducing solutions that prevent individual citizens from making their own informed decisions about risk.

The above harms highlight the importance of a principles-based approach to cybercrime capacity building, which section delves into further, one that is also human-centric approach to protect against such harms.

Section 2: Article 86 on General Principles of Technical Assistance

'Principles for cyber capacity building' is not a new concept. The Global Forum on Cyber Expertise (GFCE) agreed principles for cyber capacity building in its 2017 Delhi Communique which, in turn, were largely built around the Busan Partnership for Effective Development Cooperation principles.[10] Additionally, research works in this area have argued that a principles-based approach to cyber capacity building would not only provide vital checks and balances for capacity building activities, but would also better align capacity building with international development.[11] Thus, the AHC's general principles on technical assistance must not be conceived of, implemented or discussed in isolation.

In fact, the OEWG's 2021 report – which was endorsed by all UN Member States – states that capacity building should be informed by 11 principles.[12] These 11 principles are organised under three categories: process and purpose; partnerships; and people. While this report and the capacity building principles were devised in relation to the state use of ICTs in the context of international security, there are important connections to the AHC process and cybercrime.

Firstly, cyber capacity building encompasses cybercrime capacity building. While cybersecurity capacity building and cybercrime capacity building contain different elements, they are intrinsically linked, and strong cybersecurity capacity building cannot be completed without a strong cybercrime capacity building component. Often, the skills, tools and knowledge-sharing that takes place are similar, if not identical.

Secondly, and subsequently (noting the first point), the principles outlined in the OEWG report should then be transferable to the AHC. Article 86 of the CND, however, outlines only three 'General Principles of Technical Assistance'.[13] Figure 1 below maps how the AHC technical assistance principles align with the OEWG cyber capacity building principles.

Figure 1: Mapping the AHC technical assistance principles against the OEWG Cyber Capacity Building principles.

General principles of TA in Cybercrime convention	**OEWG Cyber Capacity Building principles**
Art 86 (1) (c) Initiatives shall follow a comprehensive and systematic approach that includes multiple levels and dimensions (technical, human, organizational, governmental and legal	**Process and Purpose** • Capacity-building should be a sustainable process, comprising specific activities by and for different actors.

[10] https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf. and 10 https://www.oecd.org/development/effectiveness/busanpartnership.htm.

[11] Patryk Pawlak and Nayia Barmpaliou, 'Politics of cybersecurity capacity building: conundrum and opportunity', *Journal of Cyber Policy,* (2017, 2:1).

[12] UN OEWG final substantive report 2021, < https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>

[13] Art 86 CND

aspects), builds on existing capacities and ensures sustainability, transparency and accountability.	• 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.
Art 86 (1) (a) Technical assistance and capacity-building shall be carried out in an inclusive manner and include all nations, with particular attention given to developing countries, and all relevant stakeholders; *Art 86 (1) (b)* Each beneficiary shall determine its own priorities, based on country specific situations and requirements;	**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.

A comparison between the AHC technical assistance principles and the capacity building principles included in the OEWG 2021 report shows that:

First, the OEWG principles are much more comprehensive than the AHC ones. The organization of the 11 principles into three categories address various dimensions of CCB efforts and have been endorsed by all UN member states. In contrast, the AHC principles are partially focused around only the first two categories (process and purpose, and partnerships) and do not refer to the People involved in these processes and activities, including human rights protection.

Second, there is a more considered attempt to award all Member States agency in these activities. The OEWG principles do not use a framing that separates developing countries from developed countries. Instead, the OEWG principles refer to active partners based on the differentiated roles and responsibilities and context. Whilst the mention of 'an inclusive manner' is welcomed, the AHC could adopt a similar framing to avoid reinforcing existing divides and capacities asymmetry between states and to give agency to all countries in the cybercrime capacity building efforts. This can help reduce the third type of harm where cybercrime capacity building can be used to reinforce dangerous or harmful international (political) power dynamics at the expense of equitable transfer of skills, expertise and knowledge.

Third, while both the OEWG and the AHC talk about gender in capacity building, the AHC would benefit from incorporating gender into its general principles for technical assistance as the OEWG has done. Article 87 (2) (n) of the CND calls for 'Methods for mainstreaming a gender perspective into policymaking, legislation and programming'. This is welcome and deserves credit, but should be supplemented with a reference to gender in the general principles in Article 86. All potential capacity building programmes listed under Article 87 should be subject to methods for mainstreaming gender sensitivity and a gender perspective. Including a reference to gender in the general principles in Article 86 would reinforce the importance of: developing capacity building activities and programmes in a way that makes accommodations for those who are historically disadvantaged or marginalized due to their gender; being aware of the inherent biases and stereotypes that manifest themselves as discrimination; and designing activities and programmes in a way that consciously and sustainably increases and improves the capacity of all people involved in delivering anti-cybercrime measures in an equitable manner.

A **shared** principles-based approach to cybercrime capacity building – or technical assistance – that builds on what has already been agreed and established in parallel UN processes can:

1. Be a better guarantee of consensus amongst Member States on how cybercrime capacity building and technical assistance should be delivered;
2. Provide a sound theoretical underpinning for how capacity building should be conducted and to what means and ends; and
3. Improve the overall efficiency of cyber capacity building and international development in general by enabling and encouraging avenues of cooperation between various capacity building and development efforts.

Section 3: Article 87 on Training and Technical Assistance

Article 87 on training and technical assistance focuses largely on areas of cooperation between Member States, which speaks to the need for levelling the playing field amongst them in order to facilitate swift and efficient cooperation.

This section examines Article 87, particularly Article 87(1) which addresses the responsibilities of state parties themselves for improving their capacity on the prevention, detection, investigation, and prosecution of offences under the convention, and compares it with a framework on Strategic

Approaches to Countering Cybercrime (SACC) that Chatham House has developed (Annex 1). The SACC framework consists of five 'pillars' that covers the cybercrime response lifecycle: strategy development, establishing the enablers, establishing operational capability, tasking and prioritization, and evaluation. Under each pillar are a set of questions that are designed to help identify gaps in cybercrime response. The framework aims to initiate a structured conversation among policymakers on how to tackle cybercrime comprehensively and strategically, which in turn can help countries develop a set of interventions that address their specific needs and priorities, identify gaps in any current or existing plans, and benefit from the established good practice and practical support available from the international community. An *inclusive* strategic approach that empowers and gives agency to women and historically marginalized groups is more effective and holistic; recognizing this, the framework also consists of questions pertaining to equality, diversity and inclusion that aim to enhance political commitments with active solutions and actions.The aim from this comparison is not to position the SACC framework as a gold standard that all states should follow, but rather to discuss cybercrime capacity building more holistically and to stress the point about the importance of a strategic risk assessment and a tailor-made approach suited to the particular contexts in which the cybercrime capacity building efforts are focused on.

Three conclusions can be drawn from this comparison:

First, the categories of technical assistance listed in 87.2 are very specific and may be difficult to keep up-to-date.

The categories of technical assistance mentioned under Article 87.2 are very focused on investigation, but not on preventative measures that can be taken by individual citizens and businesses to reduce their exposure to cybercrime. While it is useful to provide some specific examples of the types of technical capabilities, a broader approach that treats capability gaps, not as a static matter but rather considers them as they emerge on the basis of perceived risk and need is more apt. This adaptable approach can better cater to the emergence of new threats, new investigative techniques, and new crime prevention measures, which is the approach taken in the SACC framework.

An alternative approach would be to provide some illustrative examples and identify how a more comprehensive and up-to-date catalogue of techniques can be maintained through ongoing dialogue within existing avenues in the international criminal justice community. This would mirror what already occurs within the CERT community, for example, with the global Forum of Incident Response and Security Teams (FIRST) and various regional CERT cooperation bodies.

As cybercrime threats evolve and change, and the nature of responses evolves accordingly, it will be important to update capacity building to respond to needs. Listing very specific categories of technical assistance in the convention may impede that.

***Second, the categories of technical assistance listed in 87.2 do not address many broader procedural issues*.**

While 87.2 does cover some of the broader categories in the SACC framework (such as "victim support"), there are several gaps. For example, in addition to a lack of focus on crime prevention measures, little consideration has been given to techniques for strategy development, crime reporting, operational tasking and prioritization, or for public/private intra-

governmental cooperation. All of these techniques are important to help ensure that resources are deployed effectively, and that best use is made of capabilities that may sit outside of a country's criminal justice community.

Third, there is little consideration given to how the effectiveness of technical assistance and capacity building programmes should be evaluated

There is mention of "evaluation" in 87.4, but this relates primarily to threat assessment, not to the evaluation of the effectiveness of the actual interventions taken to address the threat. Evaluation is an important capability that states need in order to manage their cybercrime resources effectively. It is also needed to ensure that technical assistance programmes deliver the desired impacts. Evaluation methodologies also provide a means for monitoring unintended harmful impacts (thereby contributing to the resolution of the issues identified in section 1 of this paper).

Evaluation is an integral part of the Busan framework, and consideration should be given to whether it should be more explicitly embedded within the AHC Principles.

Conclusion

Concerns around the convention have primarily focused on how an expanded scope of criminalization that legitimizes political and information control and how procedural powers that lack safeguards can harm, violate and undermine human rights. However, as this paper has shown, efforts to build cybercrime capacity can also cause harm intentionally or unintentionally. As such, Member States – whether they are receiving, delivering or funding – have the responsibility to ensure that these efforts are done in a human rights-respecting way to protect against the identified harms and ensure that the skills and tools gained through capacity-building are not deliberately abused or misused. This could include establishing guidelines and best practices for training and equipment provision, putting in place oversight mechanisms to monitor how these resources are used, and providing human rights training to law enforcement agencies.

Furthermore, Member States should ensure that any funds provided for cybercrime capacity-building are used in a human-rights-compliant manner. This could include conducting a human rights risk assessment and supporting a role for civil society organisations to monitor the delivery of these efforts for any human rights risks.

Capacity building is an integral part of the effective implementation of the proposed convention but must not be considered in a vacuum. A vast history and an engaged international community invested in capacity building exists and continues to grow, contributing to centralising capacity building as an international development goal and as a means for reducing cybercriminal activity globally. Connecting these elements and maximising on capacity building work done in other areas will be imperative for the AHC community to ensure effective international cooperation against cybercrime.

Annex 1: The Strategic Approach to Countering Cybercrime (SACC) framework

- Strategy development	
Strategic risk assessment	• What are the strategic risks that the country faces from cybercrime? How are these affecting its broader national, social, political and economic development objectives? • What is considered a cybercrime in the country? • What are the country's particular national priorities when it comes to cybercrime? • What mechanisms are in place to ensure that the needs of the most vulnerable groups are being addressed? • How have risks been identified and have the relevant stakeholders been involved in this process? • What are the social, political and cultural barriers to realizing equality, diversity and inclusion (EDI) commitments and considerations?
Formal documents and strategies	• What documents reflect the country's strategic approach to dealing with cybercrime? • Is cybercrime addressed in the cybersecurity strategy (if one exists)? How is it addressed in other national-level strategies (e.g. crime, national security, digital development)?How does the country's strategic approach to cybercrime address the needs of these other strategies? • What are the principal lines of activity in existing cybercrime or cybersecurity strategy documents and how do they collectively address the risks? • How have these principal lines of activity been identified? Have the relevant stakeholders been involved in this process? • Has a human rights impact assessment been applied to the country's cybercrime strategy? • How are existing obligations to EDI-related international commitments – including the Sustainable Development Goals – accounted for in the cybercrime strategy?
Cybercrime strategy governance	• Who is accountable for delivering the strategy? • Is the strategy accompanied by an action plan? • How are actions funded? • How is progress monitored and how is success defined?
Communication plan	• Has the cybercrime strategy and action plan been documented? • How is this communicated to relevant stakeholders and the public? • How is the effectiveness of the communication plan evaluated? • Does the communication plan take EDI considerations into account? For example, have efforts been made to ensure effective communication to people who are less digitally literate or have access to fewer information sources?
- Establishing the enablers	
Substantive legislation	• How is cybercrime currently defined or scoped in substantive legislation? • What laws have been placed on the statute book to cover cybercrime in the past 20 years? • Have laws been based on any international or regional conventions or standards?

	• What are the gaps in substantive legislation and how are they being addressed? • To what extent are laws, regulations and policies developed in a way that integrates EDI considerations and meets EDI commitments?
Procedural legislation	• How is procedural law used to investigate and prosecute cybercrime? • What measures are in place to ensure that criminal investigations take proper account of the particular needs and concerns of women and other marginalized groups? Which procedural powers have proved most useful in cybercrime investigations? • What are the major gaps in procedural processes (e.g. obtaining data/evidence from overseas)? • What other powers do the government and criminal justice authorities have to prevent and/or investigate cybercrime (e.g. regulatory requirements for businesses)? • What safeguarding and due diligence measures are in place? • How has legal infrastructure historically handled cases of cybercrime for people from marginalized groups?
Operational mandates	• Which are the main agencies involved in the prevention, detection, investigation and disruption of cybercrime? • What mandates or remits do they have to conduct this work? • How is the work of operational agencies overseen, e.g. to monitor performance and to avoid overreach or inappropriate application of powers? • What mechanisms for remedial actions are necessary and available for victims of cybercrime? • Which stakeholders should be included in consultations to determine whether updates to the legislative framework (e.g. a new law, or amendments to an existing law) are needed, and to ensure the reporting burden is not placed wholly on the individual?
- **Establishing operational capability**	
People and skills	• What human resources are currently deployed against cybercrime? • How are skills requirements determined, and what training do practitioners receive? • How is the required level of resourcing determined, and how is this paid for? • What standard operating procedures have been developed to guide cybercrime investigations, and how are these promulgated? • How is training focusing on the needs and characteristics of the most vulnerable victims? • How are EDI considerations integrated into hiring and training practices?
Technical capabilities	• What are the key technical capabilities required (e.g. digital forensics, data analysis, malware analysis, open source, financial investigation) and which agencies, entities or organizations (in the private and public sectors) are responsible for providing these? • What are the key technical capability gaps and how are these being addressed? • What other capabilities (technical and non-technical) are being applied to cybercrime investigations?

	• What kind of planning and preparedness programmes are in place to prepare key stakeholders for major cybercrime incidents?
Crime prevention measures	• What are the key cybercrime prevention measures and who is responsible for implementing these? • What public awareness activities are in place and how are these delivered? • What is done to protect potential victims? Which stakeholders are involved (e.g. technology firms and the retail and financial sectors)? • How has EDI been considered in crime prevention measures?
Intra-governmental collaboration, public–private partnerships and international collaboration mechanisms	• What role do governmental agencies other than law enforcement agencies (e.g. computer emergency response teams (CERTs), financial intelligence units, security agencies) play in combatting cybercrime and how is this coordinated? • What role does the private sector play in preventing and/or investigating cybercrime? • How are operational activities coordinated with various stakeholders? • What role, if any, is played by communities, schools and small businesses? • To what extent are joint operations with foreign partners, and/or regional or international organizations undertaken? • How is this collaboration enabled, and is participation in international networks facilitated (e.g. INTERPOL I-24/7)? • To what extent is the country engaged in international discussions on cybercrime policy and strategy, and how does the country ensure that its needs are being acknowledged and addressed? • In addition to outreach to relevant industries, how can longer-term and structural barriers to realizing EDI be addressed?
- Tasking and prioritization	
Setting top-level operational priorities	• How are the strategic objectives of the country's national cybercrime strategy translated into tactical objectives for operational agencies? • Who decides the balance between reactive and proactive interventions? • How does the country balance the requirements coming from local crime reporting, national organizations (e.g. ministries, security agencies, regulators) and international partners?
Intelligence and threat assessment	• How is intelligence used to drive tactical priorities? • How is intelligence used to assess the overall social and economic impact of cybercrime on the country? • How is intelligence from regional and international partners used? • What data and independent evidence on cybercrime need to be monitored and collected in order to meet EDI commitments?
Crime reporting and victim support	• How do victims of cybercrime report incidents? • What happens to these crime reports? • What support is available and provided to cybercrime victims? • What kinds of crime statistics are generated by these processes, and how are they used? • Are these crime statistics disaggregated by intersecting characteristics and identities?

	• What measures are in place to ensure that the data is treated in a confidential and sensitive manner?
Tasking processes	• On what basis is an operation or investigation initiated? • How are individual operations/investigations prioritized and tasked? Who decides? • What standard operating procedures are in place to support cybercrime-fighting activities?
- **Evaluation**	
Operational	• How is the effectiveness of individual operations and investigations measured? • Does monitoring and evaluating involve multi-stakeholders, including those working with/supporting victims and advocating for women and other marginalized groups? • Are monitoring and evaluation processes accessible and subject to EDI commitments?
Tactical	• How is the success of the individual actions within the cybersecurity/crime strategy (and any associated action plans) measured?
Strategic	• How is the impact of cybercrime on the country measured or understood, and how would a country determine if that impact has been reduced? • How is the overall effectiveness of the strategy on reducing the impact of cybercrime in the country measured? • Is the specific impact on reducing harm on vulnerable groups measured?
Strategic review	• How are the outputs of the evaluations used to improve the response to strategic cybercrime risks? • Is evaluation done with a view to assessing protection for and justice delivered to the most vulnerable?
Exercising	• Is there an exercising programme in place and if so, what is its key objective?