CHATHAM HOUSE

Integrating gender in cybercrime capacity-building

A toolkit

International Security Programme
July 2023
Rebecca Emerson-Keeler, Amrit Swali and Esther Naylor

Preface

Integrating gender in cybercrime capacity-building has been designed to provide capacity-builders with the tools to integrate gender considerations into cybercrime capacity-building programmes and activities. Built around four of the five pillars of Chatham House's Strategic Approach to Countering Cybercrime (SACC) framework, this toolkit sets out proactive and actionable steps designed to ensure the gender-sensitive design and implementation of a wide range of cybercrime capacity-building activities.

This toolkit is part of a multi-year project, funded by Global Affairs Canada, aimed at building anti-cybercrime capacity in Southeast Asia.

Contents

Introduction

The impacts of cybercrime on women, LGBTIQ people and other minoritized communities undermine progress on gender equality and contribute to global insecurity. Cybercrime defences must therefore ensure appropriate and proportionate protection for all vulnerable groups.

Gender and cybercrime – why does it matter?

Cybercrime has **gendered impacts** in several ways. For example, ransomware attacks on healthcare systems could expose data and information that render women and other marginalized groups vulnerable because of societal discrimination. Disruptions to online systems governing public services can have a negative impact on access to vital services – such as sexual and reproductive health services – for those who already face existing barriers. The hacking of social media accounts and the unlawful accessing of personal information could put marginalized individuals at risk in their communities. The negative impacts are extensive and non-exhaustive: they undermine progress on gender equality and contribute to global insecurity.

Strong cybercrime defences must be **gender-sensitive** to ensure appropriate and proportionate protection for women, **non-binary** and **gender-nonconforming** people and other vulnerable groups. At the same time, those tasked with delivering cybercrime defences must be **gender-aware**. Integrating gender in ongoing and adaptable anti-cybercrime efforts – such as capacity-building – is one way to aid that.

What can cybercrime capacity-building do?

The UN defines capacity-building as 'the process of developing and strengthening the skills, instincts, abilities, processes and resources that organizations and communities need to survive, adapt, and thrive in a fast-changing world'.

This toolkit defines capacity-builders as experts and national, regional and international organizations working on developing, implementing and strengthening cybercrime measures. The toolkit is designed to ensure that everyone responsible for developing and strengthening the skills, abilities and resources of organizations and communities to survive and thrive in cyberspace – and those who support them – does so with due regard for **gender equity and sensitivity**.

About this toolkit

This toolkit has been designed as a starting point for practitioners working on integrating gender considerations in anti-cybercrime capacity-building activities, and incorporates example projects illustrating the steps involved in planning, implementation and evaluation phases.

This toolkit will introduce capacity-builders to core concepts that are foundational to designing activities in a gender-sensitive way

What is the toolkit and who is it for?

This toolkit aims to provide both domestic and international capacity-builders engaged in combating cybercrime with actionable recommendations for ensuring the meaningful and practical inclusion of gender equity and sensitivity into their activities. Building on example projects as well as existing international resources and literature, this toolkit will introduce capacity-builders to core concepts that are foundational to designing activities in a gender-sensitive way.

This toolkit is intended as a starting point for guidance on integrating gender considerations into capacity-building activities; as such, it is not all-encompassing. There is no universal approach to gender equity and sensitivity, and this toolkit does not presume to cover gender in a way that captures all cultural and regional variances. Additionally, the practice of incorporating gender in cybercrime capacity building is dynamic: as more and more empirical data on gendered harms and discrimination is gathered, and as technology develops, our understanding of how these harms are mitigated in capacity-building activities needs to evolve. The meaningful incorporation of gender equity and sensitivity into capacity-building efforts is a continuous endeavour, and must account for local contexts.

The Strategic Approach to Countering Cybercrime (SACC) framework

The practical sections of the toolkit are built around four of the five pillars of cybercrime capacity-building, as developed under Chatham House's Strategic Approach to Countering Cybercrime (SACC) framework.

The SACC framework has been developed by researchers in Chatham House's International Security Programme to help countries understand how cybercrime is perceived, and what the main enablers of and barriers to a strategic approach to fighting cybercrime – specific to a particular country – might be. The framework is intended to support any country in developing an effective and strategic

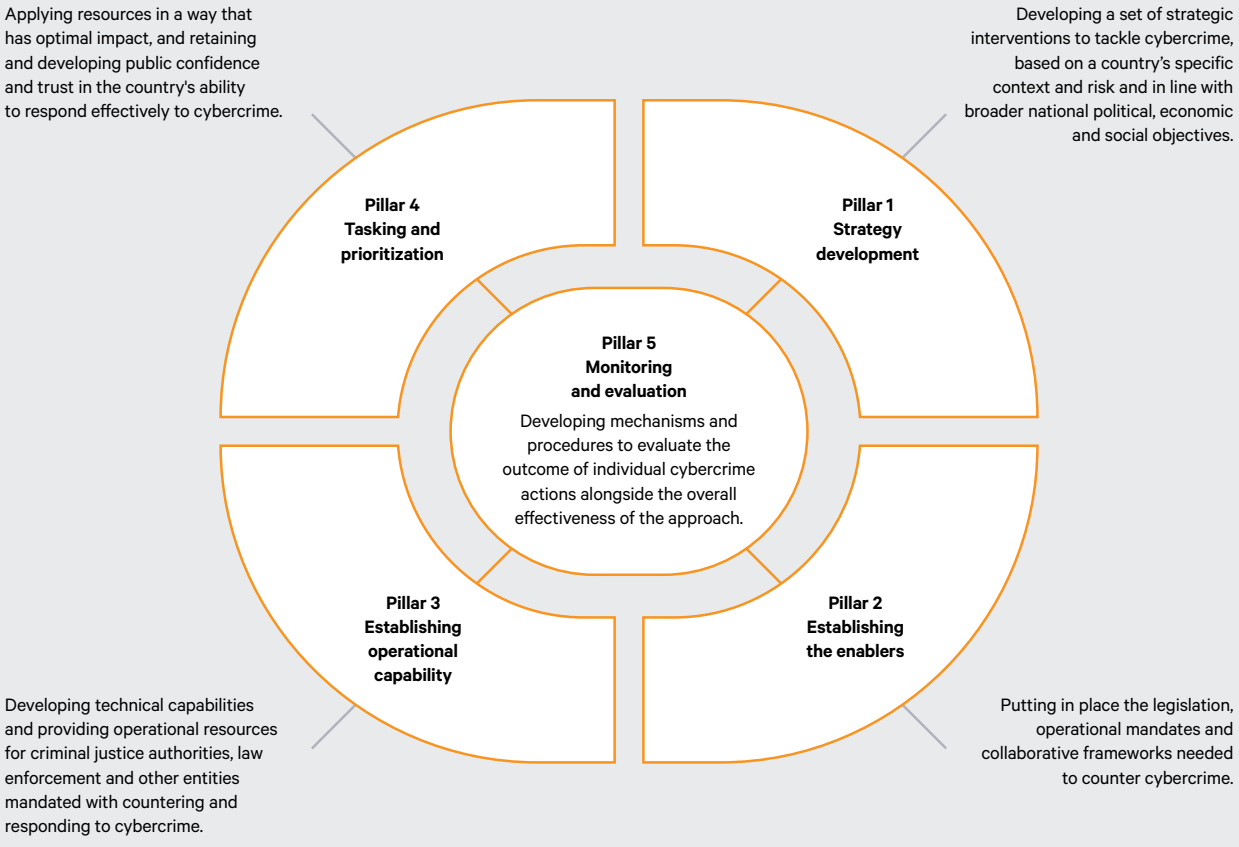
approach to cybercrime through helping it to: develop a set of anti-cybercrime interventions that address the country's specific needs and priorities; identify gaps in its current plans; and benefit from the established good practice and practical support available from the international cybercrime-fighting community.

The SACC framework has five pillars that focus on the whole life cycle of a cybercrime national response. Four of the pillars are considered in this toolkit. They are:

- Strategy development
- Establishing the enablers
- Establishing operational capability
- Tasking and prioritization

These four pillars have been identified for their relevance and applicability to capacity-building efforts. The SACC framework also includes a fifth pillar on evaluation, exploring how the effectiveness of a country's activities at the operational, tactical and strategic levels is evaluated, and how this information is used to improve that country's strategic response to its cybercrime risks. This does not feature as an independent pillar in the toolkit, which instead incorporates evaluation within each of the four pillars considered, with concrete recommendations for gender integration.

The Strategic Approach to Countering Cybercrime (SACC) framework



Working through the toolkit

The next section explains the importance and value of conducting a gender analysis of the cybercrime threat landscape. Subsequent sections then go on to introduce users to each of the four SACC framework pillars that lie at the heart of the toolkit, setting out the importance of gender equity and sensitivity to that pillar, followed by a detailed guide to integrating gender in activities that fall under that pillar.

For each pillar, the toolkit uses an example project to illustrate how gender considerations can be integrated in cybercrime capacity-building efforts. Each example project is set out in three phases: planning, implementation and evaluation. Each phase outlines a set of steps for progressing the example project, and steps for integrating gender considerations.

The example projects provided are inspired by international guidance on cyber capacity-building, and have been chosen for their relevance to the corresponding pillar and the range of gender considerations this could cover.

The example projects point to some of the ways that gender considerations can be integrated in cybercrime capacity-building. The examples are illustrative, and the gender considerations outlined can be applied to other projects or activities under that pillar.

The toolkit also includes a glossary section, in which key terminology (highlighted in bold in the toolkit text) is defined, as well as a list of further resources for users to explore.

Undertaking a gender analysis

In the context of cybercrime capacity-building, a gender analysis is an assessment of how – if at all – policymakers think about gender and online security, and how this is reflected in policies.

What is a gender analysis?

The UN defines gender as 'the social attributes and opportunities associated with being male and female and the relationships between women and men and girls and boys'. While definitions of gender vary, it is commonly understood that gender exists on a spectrum and is socioculturally constructed, with the result that it often mirrors power hierarchies and dynamics. The word 'gender' is not synonymous or interchangeable with 'women'.

The word 'gender' is not synonymous or interchangeable with 'women'

A gender analysis is a way of understanding the way gender is conceived and understood in a particular context, and the impact it has on people's experiences in that context. It reveals key information around the power dynamics and perceptions of inclusivity among people based on how they identify. A gender analysis provides information that recognizes both the impact of gender and its relationship with race, ethnicity, culture, class, age, disability and/or other status. At a basic level, and for capacity-building purposes, a gender analysis is an assessment of how – if at all – policymakers think subconsciously and consciously about gender and online security, and how this is reflected in policies.

Why is it important to undertake a gender analysis?

Organizations and the people they serve have differing perceptions of their security, based on gender and other characteristics. Analysing security threats is the best way of forming strategies for proactive and reactive security. Strategically strengthening confidence, trust, security and reliability of information and communications technologies (ICTs) and of ICT systems through a **gender lens** facilitates more equitable economic development, access to vital and transformative

public services, and the sharing of information. It also improves overall operational effectiveness.

To develop a strategic picture of the cybercrime landscape, it is important to recognize that different people experience and receive cybercrime and responses to cybercrime in different ways, including on the basis of their gender, sexual orientation and other **intersecting identities**, and depending on the political, social and cultural context. Furthermore, the impacts of security policies and strategies are not equal across different groups and often magnify existing gender inequalities. Undertaking a gender analysis of the cybercrime landscape helps capacity-builders identify risks and harms that can be **gender-disaggregated** to increase the opportunities for operational effectiveness in developing activities to combat cybercrime.

How do I undertake a gender analysis?

It is important to ask what data are missing and why; some cybercrime victims may be reluctant to report or may be unaware of reporting mechanisms and resources

There are several starting points for undertaking a gender analysis. The following examples are not exhaustive, and should be context-driven:

Employ a gender and inclusion consultant

Undertaking a gender analysis may require expertise beyond what already exists within an institution. Working with a gender and inclusion consultant is an effective way of navigating **gender equity and sensitivity** in a way that is appropriate and relevant to the immediate environment. A consultant will have expertise in, and be aware of, resources, tools and frameworks that can help conduct a gender analysis in a methodological way. A consultant can also add an 'external' lens that can encourage a more objective assessment of the institution and its activities. Gender and inclusion considerations are not always applicable across sectors or themes, but the principles are similar. Although some proficiency in cyber will be beneficial, it is not necessary for a gender and inclusion consultant to be a cybercrime expert in order to add value.

Gather cybercrime data

When undertaking a gender analysis, it is important to collect data pertaining to gender and cybercrime more broadly and then disaggregate the data by gender, age, ethnicity, class, socio-economic background and other relevant intersecting identities. This can help to identify trends relating to the types of crimes, victims and perpetrators, and the harm experienced. It is also important to ask what data are missing and why; some cybercrime victims may be reluctant to report or may be unaware of reporting mechanisms and resources. Where possible, the collection of data should be standardized to ensure efficiency in collating or combining data across multiple agencies and/or organizations.

Engage relevant stakeholder groups

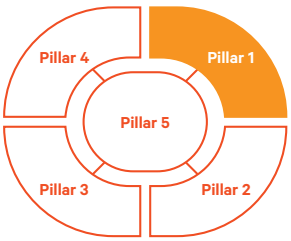
Engaging with gender and human rights groups, academics and community leaders helps stakeholders to fill any gaps within the gender analysis, and to understand local and contextual gender dimensions. Stakeholders should (if possible) be formally involved to advise, provide evidence or insight where data are missing, or to complement data.

Identify where gender is stated as a national priority

If gender is stated and acknowledged as a national priority, it is easier to make the case for mainstreaming gender into anti-cybercrime activities. An audit of national priorities – in constitutions, treaty commitments, manifestos, etc. – should be conducted to identify where there are actions and statements in place that reflect the importance of gender equality, equity and/or sensitivity in policies and frameworks. This might include assessing the capacity of the institutions or departments responsible for countering or responding to cybercrime to embed gender and inclusion in their mandates. It might also include assessing whether institutions leading on cybercrime response, prevention and mitigation have meaningful equality at all levels in their administration, and whether there are barriers to the involvement of certain groups.

Pillar 1: Strategy development

This section examines why gender is important in strategy development – including how strategic risks and priorities are perceived, identified and assessed. An example project illustrates the steps involved in integrating gender when developing a national cybercrime strategy.



What do we mean by strategy development?

Strategy development looks at what already exists in-country by way of formal or informal cybercrime strategy, how this was developed, and what programmes/activities have been put in place to support the implementation of that strategy. This pillar explores how strategic risks and priorities are perceived, identified and assessed at the national level – particularly with regard to their impact – and the extent to which these are captured within a formal document (or documents), be this a cybercrime strategy, part of a cybersecurity strategy or other relevant documentation. Strategy development further includes the evaluation mechanisms in place to assess the effectiveness of the strategy's delivery and communication.

Projects that focus on strategy development include (but are not limited to):

- supporting the development of a cybercrime strategy;
- implementing a cybercrime strategy;
- developing best practice recommendations for cybercrime strategies; and
- reviewing and assessing a cybercrime strategy.

Thinking about gender and strategy development

Gender is important for strategy development because decisions about how to design, build and use tools to respond to and/or mitigate the impacts of cybercrime have different effects on different people and communities. Globally, not only

are women and other marginalized groups under-represented in the governance and regulation of ICTs, but **gendered impacts** are often overlooked.

Frequently, agencies or governments do not have the capacity or resources to meaningfully integrate gender analysis or expertise within their workflows

Frequently, agencies or governments do not have the capacity or resources to meaningfully integrate gender analysis or expertise within their workflows, let alone to allow for sharing ideas, experience and best practice with other ministries or agencies. Increasing both capacity and resources can aid the development of better coordinated processes that tackle gender concerns as innate to cybercrime policy planning.

In thinking about gender and national cybercrime strategies, policymakers need to ensure that silos among bodies such as local law enforcement, judiciary, national crime agencies, government departments and civil society organizations working on advancing human rights are broken down, and that narrow perspectives on what constitutes gender are challenged.

Key questions

Here are two key questions to consider when integrating gender into strategy development:

- What are the existing obligations to international commitments – such as the Women, Peace and Security (WPS) agenda, the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and the Sustainable Development Goals (SDGs) – that seek to protect and promote the rights of women and other marginalized groups?
- What are the local social, political and cultural contexts, and what are the barriers to realizing the rights and security of women and other marginalized groups?

Example project: developing a national cybercrime strategy

This section uses an example project to show how gender can be integrated in strategy development. The example given considers the development of a national cybercrime strategy.

Planning

1 Set the stage

When developing a national cybercrime strategy, the objectives should be clear from the start. This includes understanding the cybercrime landscape in a particular country, setting out what the strategy is going to achieve – and how – and highlighting the benefits of having a written strategy.

- **Gender-responsiveness** should always be explicitly integrated within the objectives of a strategy. This means that there should be a stated commitment to combating the **gendered impacts** of cybercrime, and to addressing harms at all stages. There should also be a clear commitment to understanding the gendered impacts of the strategy itself, which will need regular re-evaluation.

2 Establish a project authority

Establishing a project authority, made up of a senior official (ideally a government minister) and a project team, with responsibility for developing, implementing and revising the cybercrime strategy will help to enable strong cooperation among multiple stakeholders.

— Decision-makers in government and the organizations to which the strategy applies must understand the operational importance of gender and cybercrime, and commit to integrating gender in strategic priorities. It is important to find allies among senior decision-makers who can help ensure gender is a priority and hold other stakeholders to account.

3 Facilitate intergovernmental cooperation

Intra-agency and intergovernmental cooperation are vital to building effective strategies. The project authority should consult all relevant partner agencies to obtain their input and support, and should establish a mechanism to ensure this cooperation.

— Engagement with agencies that have historically mainstreamed human rights and gender equality in their work – through mandates or as best practice – must be integrated in governance mechanisms, along with law enforcement agencies and judicial authorities that focus on issues of violence against women and girls, child protection, support for people with disabilities, and human-trafficking. This integrated approach means that the requisite expertise and operational knowledge are available for developing a strategy.

4 Conduct stakeholder consultations

An iterative process is needed to identify the focus areas of the strategy, and to allow stakeholders to provide input on how progress can be made and how the strategic objectives should be shaped.

— Stakeholder consultations are a fundamental component of understanding the cybercrime and gender landscape. It is essential to assess the offline needs and experiences of women, men and LGBTIQ+ people across public, private and civic space. It is also critical to recognize that offline harms manifest in the online space, and that gender-based harms are under-criminalized, resulting in dangerous and serious omissions in cyber strategies.

5 Allocate gender resources and activities in the budget

A dedicated budget and resources are vital to a successful project. This includes dedicated project staff who are trained in the operational aspects of developing national strategies or policies, and staff who have cybercrime expertise from across sectors or departments. The budget must also consider costs beyond staff and resources, including services and communications.

— Implementing a cybercrime strategy with an integrated approach to gender requires adequate resources from the outset. Undertaking a gender analysis of the cybercrime landscape allows for resources to be allocated appropriately by revealing what is feasible, what exists, what is lacking, and the financial costs involved.

— Financial allocation should ensure that a specific – and, where possible, ambitious – budget is in place to address gender-based needs. This budget should take into account the size and scale of the project, the services and activities that will be necessary to accommodate the needs of the target groups, and provisions for building team capacity on gender and inclusion.

— Possible costs, in addition to engaging a gender expert, might include those of communications to reach women, girls and LGBTIQ+ people on safe and relevant platforms.

Implementation

6 Designate the steering committee

The creation of a steering committee allows for formal, regular and accountable multi-stakeholder engagement. The steering committee should include the project authority, relevant senior-level officials (including in law enforcement agencies and the judiciary) and non-governmental stakeholders selected for their ability to provide strategic oversight and guidance at the different stages of the cybercrime strategy life cycle.

The steering committee should be made up of a proportional representation of women, men, non-binary or gender-nonconforming people, and LGBTIQ+ people

— Gender equity and responsiveness should be meaningfully integrated in the terms of reference of the steering group. This is an important step for accountability.

— The steering committee should be made up of a proportional representation of women, men, **non-binary** or **gender-nonconforming** people, and LGBTIQ+ people. Barriers to participation should be explicitly considered and addressed: this might include making provision for childcare for parents working out of hours, disability access, or interpretation to account for linguistic diversity. The steering committee should also draw on effective intergovernmental cooperation on gender equality.

— There should be designated positions on the steering committee for gender-mandated departments or agencies (and/or human rights-mandated departments or agencies), including those involved in victim support.

7 Conduct stocktaking, assessment and analysis

It is crucial for a country to take stock of its available processes, resources and skills to combat cybercrime, and identify where there are deficiencies. This stocktaking might focus on staff working on cybercrime response activities, the mechanisms and procedures those staff use to do their work, and the legislative and regulatory environment in which they operate.

— Most auditing work will have been completed when undertaking a gender analysis of the cybercrime landscape. However, it is also important to audit the capacities and capabilities of lead agencies with regard to gender.

— As part of this auditing work, stakeholders and their respective roles and responsibilities need to be mapped to assess whether they have gender expertise integrated in their organizational priorities and strategies.

— Consultant specialists should be brought in to aid implementation and help deliver a self-assessment of gender needs.

— Capacity should then be built up to address identified needs; and experience, expertise and best practice may usefully be shared with other departments.

8 **Assist in the drafting of the cybercrime strategy**

Based on internal and external consultations, feedback and reviews, a cybercrime strategy should undergo several stages of rewriting during the drafting process to ensure all appropriate needs are being met and relevant concerns are being addressed.

Using platforms that reach audiences from under-served backgrounds and communities is fundamental to ensuring the published strategy is disseminated beyond practitioners and politically engaged actors

— Gender-sensitive drafting is the practice of producing a strategy that is sensitive to gender inequalities and gendered experiences of cybercrime. Evidence from the gender analysis of the cybercrime landscape should be used to ensure different strategic areas are being appropriately considered and the right concerns are being addressed.

— Language and content should be checked for gender sensitivity. A gender adviser or consultant can do this.

— To ensure accountability, key commitments on gender and inclusion should be shared with stakeholders and the public. Using platforms that reach audiences from under-served backgrounds and communities is fundamental to ensuring the published strategy is disseminated beyond practitioners and politically engaged actors. This can be done by, for example, translating the content into other languages, or making materials accessible to those without access to technology.

Monitoring and evaluation

9 **Assist in the monitoring and evaluation of the strategy**

Monitoring and evaluation should be undertaken by the project's governance structure, and should take place at regular intervals. Recommendations arising from these evaluations should be incorporated in revisions to the strategy, and insights and data should be shared with relevant stakeholders.

— Monitoring and evaluation should include the gathering and disaggregating of gender-based data to understand the impact of the strategy on various populations and communities. Conducting interviews or consultations with affected communities is another important way of bringing visibility to what data may not reveal. All data should be treated sensitively and in confidence, in line with all relevant data protection legislation.

— Where possible, data collection should be standardized across agencies; data are easier to combine and analyse if they are all in the same format.

— Monitoring and evaluating should also include a financial assessment to understand whether resources have been sufficiently allocated and needs met. Outcomes should be assessed according to success, and in line with objectives outlined at the start of the process.

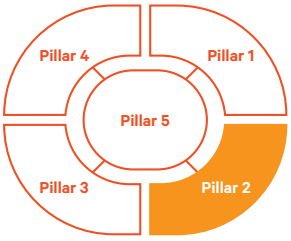
10 Assist in making strategic adjustments

The cybercrime strategy should be periodically reviewed to keep pace with technology developments, new forms of cybercrimes, and the evolving needs of the country.

— Outcomes should be regularly assessed to understand changes to the impact of cybercrime and the cybercrime strategy on women and other marginalized groups. Emerging technologies – and international policy frameworks designed to regulate them – will also need to be considered and assessed for gender-based harms.

Pillar 2: Establishing the enablers

This section considers why gender is important to the development of 'enablers' such as anti-cybercrime laws and agencies. An example project illustrates the steps involved in integrating gender when developing a cybercrime law.



What do we mean by establishing the enablers?

Establishing the enablers for combating cybercrime considers the funding, legislation and mandates that are in place to support delivery of effective cybercrime interventions. It includes the necessary legislative measures that address cybercrime substantively and procedurally, and their relation to regional and international legal instruments. It also covers the agencies involved in tackling cybercrime and their mandates, as well as the checks, balances and safeguards that are already in place to ensure mandates are not breached and powers not abused.

Projects that focus on establishing enablers include (but are not limited to):

- developing or reforming cybercrime laws;
- harmonizing legislation at regional and international levels;
- implementing cybercrime laws; and
- establishing a dedicated cybercrime agency.

Thinking about gender and establishing enablers

Gender is important for establishing enablers because national legislation, policies, regulations and organizational mandates to address cybercrime need to be systematically and structurally sensitive to the specific vulnerabilities

and threats faced by women and other marginalized groups. There are several international instruments that outline governments' obligations to protect the rights of women, people who are **non-binary** or **gender-nonconforming** and minority groups.

It is important to recognize that cybercrime legislation and regulation can be used as a tool to limit the exercise of rights and freedoms

However, discriminatory spaces do exist at national, regional and international levels. Creating gender-sensitive enabling frameworks against cybercrime requires addressing discrimination and navigating **gender-blind** spaces in order to close gaps. It can also provide opportunities to refocus efforts to uphold state obligations to people who are vulnerable to discrimination or violence based on their sexual orientation or gender identity. Equally, it is important to recognize that cybercrime legislation and regulation can be used as a tool to limit rights and freedoms: this is already disproportionately experienced by women, LGBTIQ+ people and people from minoritized groups.

Cyber-dependent crimes and **cyber-enabled crimes** all have gendered impacts. Although what is illegal offline is also illegal online, capacity-builders should appreciate that gender-based crimes and violence are under-reported and that access to justice is often constrained globally. By ensuring that enablers are robust, and meet – at a minimum – the needs of women and other marginalized groups, existing frameworks can be strengthened.

Key questions

Here are some key questions to consider when integrating gender as part of establishing enablers:

- What national, regional and international commitments and obligations exist to protect the rights of women and other marginalized people, and what are the structural and/or cultural barriers that prevent the realization of these rights?
- How has legal infrastructure traditionally and historically handled cases and incidents of cybercrime for men and for women, LGBTIQ+ people and other marginalized communities?
- How can laws, regulation and policies be developed in a way that protects meaningful digital access and rights?
- 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 (i.e. a new law, or amendments to an existing law) are needed, and to ensure the reporting burden is not placed wholly on the individual?

Example project: developing a cybercrime law

This section uses an example project to demonstrate how gender can be integrated when establishing enablers. The example given considers the development of a cybercrime law that is focused on reducing harms caused by cybercrimes.

The starting assumption is that a country does not currently have a cybercrime law in place. However, the gender recommendations in this project also apply to the amendment of existing laws, which might be **gender-blind** or exacerbate gender inequalities.

Planning

1 Set the stage for the cybercrime law

It is important to understand where the proposed cybercrime law sits within the strategic national cyber landscape and legislative framework. The cybercrime law may be part of a broader cyber strategy and accompany a suite of measures designed to fight cybercrime. It will often act as an enabler of many of the goals and objectives contained in the strategy.

There is often limited information about the impact of laws and law enforcement on women and other marginalized groups

- It is important to assess whether existing legislation takes account of the gendered impacts of laws on, for example, data protection, intellectual property, etc.
- Offline discriminatory legal norms (such as the criminalization of gender identity issues on social or cultural grounds) may be amplified in cyberspace, and issues may arise when the drafting of legislation on cybercrime refers to wider laws. Recognizing this at the start can set the scene for sensitive drafting.

2 Identify the legislative lead

Draft national cybercrime laws can be developed by a variety of actors. However, they are commonly developed by the interior (i.e. home affairs) and/or justice ministries, whose remit covers law enforcement and, increasingly, technology-related crimes. The legislative lead should come from one of these ministries, but should have experience of specific anti-cybercrime measures falling within the purview of the different ministries.

- The legislative lead should include people with varying expertise and knowledge. This includes gender-sensitive judicial drafting expertise, as well as experience of and expertise in working with victims and survivors.

3 Undertake an assessment of existing legislation

Most countries will cover some form(s) of cybercrime in existing legislation. Given the evolving nature of technology, these pieces of legislation will need to be periodically reviewed and updated as necessary. Therefore, it is important to understand what legislation exists at national, regional and international level, and whether this is being used appropriately and has sufficient resources for effective implementation, in order to contextualize and justify the need for any new legislation.

- There is often limited information about the impact of laws and law enforcement on women and other marginalized groups. There are three elements that are important to consider when undertaking an assessment of existing legislation:
  - What are the gendered dimensions of cybercrime that are most relevant to the context?
  - What are the gendered impacts of existing laws that seek to criminalize violence and/or abuse against women, non-binary or gender-nonconforming people and marginalized communities, and do these laws incorporate measures for online crimes? Do these laws work for diverse groups of people?
  - What are the tensions between rights within this context, for example, when freedom of expression is cited?

4 Consult model guidance for drafting the cybercrime law

Some regional and multilateral organizations have developed 'model' laws and projects designed to help countries draft national cybercrime legislation. The models include examples of key definitions, and also detail various elements of cybercrime laws, including substantive and procedural legislation and international cooperation. These are a starting point, however: the final law should be developed to meet the specific needs of the national cybercrime landscape.

Use gender analysis tools alongside legal drafting guidance, with the goal of mitigating potential harmful interpretation or misuse

- Legal drafting guidance often suggests that the drafting process should be gender-neutral. However, legal drafting should also be gender-sensitive. This means ensuring that cybercrime legislation is designed in a way that effectively meets the needs of women and other marginalized groups.
- When consulting model guidance for drafting a cybercrime law, be aware that many of the models do not incorporate gender considerations. It is important to use gender analysis tools alongside legal drafting guidance, with the goal of mitigating potential harmful interpretation or misuse. All cybercrimes will have a gendered impact, and the legislation should reflect these nuances.

Implementation

5 Assist in the creation of a first draft of the cybercrime law

A first draft of a cybercrime law should undergo several stages of drafting, internal and external consultation, review, feedback and amendments on the part of national stakeholders.

- Before articulating protections, laws need first to acknowledge positions of inequality. This means recognizing that people have differing levels of access and rights in cyberspace depending on their gender identity or sexual orientation. Gender-sensitive legislative drafting does not mean using terms like 'gender' or 'women' repeatedly. Instead, it means referencing and acknowledging:

- the different needs and experiences of people related to their characteristics and how they identify;
- the targeting of individuals that happens in the online space, based on these characteristics; and
- the need to work, from the outset, with intermediaries such as civil society and community groups, in order to relieve the reporting burden on women and other marginalized groups.

— The drafting process should include diverse stakeholder feedback forums, with representation from rights practitioners, lawyers and academics. Additionally, in consultation with civil society and women's groups, a common terminology should be developed to ensure that gender terms, definitions of gender-based harms and acronyms are agreed, sensitive and well understood.

6 Assist in conducting stakeholder consultations

Once the draft has been tested and validated with national stakeholders, public, written feedback should be sought from a broader range of stakeholders. This will help to ensure that a wide range of stakeholders have been consulted, and that all important issues have been covered, before the law is finalized.

— Stakeholder consultations contribute to overall transparency of legislative development and improve inclusivity in decision-making, ultimately strengthening the rule of law.

— Stakeholders working with, for example, survivors of cybercrime (including online abuse) can provide important information about the legislative impact of laws, and the gaps in existing laws, to ensure that future laws are drafted appropriately. These groups should be consulted when drafting a cybercrime law, and feedback loops should be developed to allow for review and amendment.

— The process of conducting stakeholder consultations should be made accessible to allow for the highest possible level of participation. This can be undertaken by running workshops or using intermediaries such as consultants or gender-mandated organizations.

7 Assist in finalizing and enacting the cybercrime law

The draft should be revised and finalized using the feedback from the consultations and existing guidance on developing cybercrime laws.

Once the draft cybercrime law has been finalized, it is ready to be presented formally for adoption and may be amended further in accordance with the national legislative process.

— Legislators will be better equipped to leverage legislation to meet the human and gendered impacts of cybercrime if a cybercrime law has been drafted to examine: gender disparities in access to cyberspace; the gendered dimensions of abuse or crime; gendered vulnerabilities; and the impact of public response to these issues.

8 **Provide capacity-building activities for national stakeholders**

The cybercrime law is likely to confer new and additional powers on law enforcement agencies, national authorities and members of the judiciary. Therefore, given the technical nature of cybercrime, it is important to consider delivering training and information materials on aspects of the new cybercrime law.

Victim support groups and other national stakeholders should understand the law, especially around victims' rights and law enforcement obligations

- Legislative bodies and government agencies that are responsible for combating cybercrime must have the capacity to deal with the nature of the law and to understand gender-responsiveness within it. When undertaking a gender analysis, it is important to understand the judiciary's history and achievements in gender equality, and to identify enabling factors and risks with regard to the legislation's potential impact on marginalized groups. Any law must be enforced in a way that does not prejudice women or other marginalized groups, and those tasked with implementing the cybercrime law should be gender-aware.
- Additionally, victim support groups and other national stakeholders should understand the law, especially around victims' rights and law enforcement obligations. Providing capacity-building activities for national stakeholders – such as women's and minorities' rights groups and national human rights institutions – will assist in identifying weak spots and ambiguities in the law, and ensure that these groups are better equipped to assist survivors.

Monitoring and evaluation

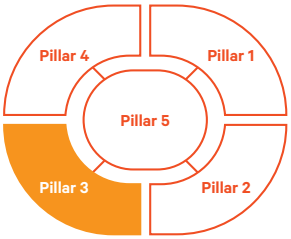
9 **Assist in planning for periodic legislative reviews**

The legislative lead should be responsible for reviewing the legislation, and for collecting and analysing cybercrime data that will inform any subsequent amendments to the law. The legislative lead should also work with law enforcement agencies, the judiciary and academics to gather data to inform, where necessary, further revisions to the cybercrime law. Legislation should be reviewed in line with analysis that takes account of an updated cybercrime threat landscape.

- While it can be difficult to accurately collect hard data and quantitative gender evidence in the cybercrime space, qualitative feedback loops can provide information on experiences, opinions and attitudes.
- Feedback loops are particularly important when engaging feminist and LGBTIQ+ organizations that may have capacity limitations. Survivor perspectives and reporting mechanisms should be incorporated through third-party consultations to ensure that the legislation can be reviewed with due consideration for the impact on the most vulnerable populations.
- These reviews must also include the experiences of people who may have limited access to the internet and online reporting mechanisms, such as the elderly, people with disabilities and/or people living in rural areas.

Pillar 3: Establishing operational capability

This section focuses on why gender is important to understanding the human and technical capabilities that exist for investigating and fighting cybercrime. An example project illustrates the steps involved in integrating gender in developing digital forensics and evidence training.



What do we mean by establishing operational capability?

Establishing operational capability considers what human and technical capabilities are in place for investigating and combating cybercrime – such as digital forensics capabilities, malware analysis, etc. – and what is missing. This pillar focuses on crime prevention measures and the allocation of roles and responsibilities. It also covers the established mechanisms for collaborating with partners in government, with the private and public sector, and with regional and international partners, and for engaging with international processes.

Projects that focus on establishing operational capability include (but are not limited to):

- developing digital forensics capabilities and digital investigations, and e-evidence training;
- cybercrime prosecution training;
- establishing public–private cooperation platforms; and
- regional tabletop and simulation exercises on crisis response.

Thinking about gender and establishing operational capability

Technology is often considered to be gender-neutral. However, ICTs including spyware and smart devices are often used to perpetrate violence against women and LGBTIQ+ people

Gender is important for establishing operational capability because when women and people who face discrimination or exclusion are involved in developing institutional responses, the human impacts of cybercrime and survivor-centred outcomes are more effectively considered. Technology is often considered to be **gender-neutral**. However, ICTs including spyware and smart devices are often disproportionately used to perpetrate violence against women and LGBTIQ+ people. Furthermore, **male-by-default designs** that reinforce gender stereotypes or that fail to accommodate the needs of marginalized groups can make it difficult to address infrastructural inequalities. Mitigating these biases and harmful impacts in operational capacity and capability is therefore all the more important.

In addition to gender equality and meaningful participation, it is important to build and enhance the knowledge, skills and ability of individuals, institutions, groups and organizations to foster advocates, perform functions, solve problems, and set and achieve gender-sensitivity objectives in ways that are both sustainable and transformative.

Key questions

Here are two key questions to consider when integrating gender in operational capacity and capability:

- What are the barriers to the early participation and retention of women in operational capacity and capability?
- In addition to outreach to industry, academia and media, how can longer-term and structural problems – such as the relatively low numbers of women in technical careers, the criminal justice system or other relevant stakeholder groups – be addressed?

Example project: developing digital forensics and evidence training

This section uses an example project to demonstrate how gender can be integrated when establishing operational capability. The example given considers the development of training for digital forensics and evidence.

Planning

1 **Set up the digital forensics training**

It will be necessary first to secure and sensitively allocate the budget, resources and delivery platform for digital forensics and evidence training, as well as the participation of expert trainers. Depending on internal capacity to deliver training, this type of training may be outsourced to an external partner.

Trainers should be able to represent diverse perspectives to ensure that content is delivered in a meaningful and accessible manner

- When setting up the training, it is important to understand potential barriers to participation for women and other marginalized people. Carrying out focus group discussions or conducting interviews with representatives of these groups already working in digital forensics will help identify opportunities and incentives. Where possible, agencies and departments might wish to nominate women or people from other marginalized groups to participate in training.
- When allocating the budget, consideration should be given to the provisions that need to be made for women, people with disabilities and survivors of digital violence – including trauma support, facilities, training in safe and accessible locations, etc.
- Trainers should be able to represent diverse perspectives to ensure that content is delivered in a meaningful and accessible manner. Requests for single-gender learning environments should be accommodated where possible. Partnering with digital rights organizations or the private sector can make accommodating these requests easier.

2 Identify the objectives of the training

Digital forensics and evidence training is becoming a standard training activity for law enforcement officers and prosecutors. The objectives of the training should be tailored specifically to those beneficiaries and to the digital forensics and evidence needs of their departments/organizations.

- The objectives of the training should be assessed with regard to the gender analysis that has been conducted to understand the cybercrime landscape. An additional risk assessment should be undertaken to consider whether the objectives conflict with **do no harm** principles for women and minority groups.
- Objectives should be based on principles to protect the survivor. These principles – and the training being developed – should appreciate that the burden to report and provide e-forensics has to be balanced against the reality that:
  - it can sometimes be difficult to trace e-evidence to the perpetrator of an **interpersonal crime**;
  - the survivor may not have retained the evidence because they fear exposure, or because their activity may not conform to social norms; and
  - the victim may not be online or have access to the evidence (e.g. in cases concerning third-party data or crimes against someone who is not digitally connected).

3 Determine the knowledge levels and skills of participants

The trainers and organizers should develop and circulate a pre-training survey to determine base levels of knowledge, technical skills and understanding among target participants, and to identify key areas to inform the delivery of the training content.

- Pre- and post-training assessments should consider the reality that men, women and people with other protected characteristics reflect on their skills, knowledge and ambition in different ways.
- Techniques to better engage women and minority groups might include focus group discussions.

4 Develop the curriculum

The trainers and organizers should develop the training curriculum based on the objectives and needs of the beneficiary. Depending on the beneficiary's needs, it may be possible to use an 'off-the shelf' curriculum that, once completed, is accredited.

- Curriculums should be developed to include gender equality and sensitivity. They should also reflect key requirements and gaps identified in the gender analysis and the previous steps.
- The curriculum should include gendered dimensions of key issues. This might include a module on gender and digital forensics, focusing on the challenges in collecting and storing e-evidence. It might also cover issues of sensitization to different digital experiences based on one's gender.
- Engaging civil society actors, academics and social media companies to help build relevant case studies into the training is fundamental. Anonymized case studies and simulation exercises can help encourage participants to address bias. As there are limited best practice examples to date, it is essential to ensure that organizational practices meet the needs and concerns of women, LGBTIQ+ people and other marginalized groups, and are amended to reflect operational realities.
- In some ministries and agencies, personnel loss also means loss of expertise. When developing the curriculum, consider whether your training will be structured to 'train the trainer'. The training should set out clearly how learning can be made sustainable and long-lasting (e.g. by sharing materials and resources with participants so that what is learned can be embedded in institutional knowledge).

Anonymized case studies and simulation exercises can help encourage participants to address bias

Implementation

5 Deliver a dry run of the training

A practice session, or dry run, will help the trainers and organizers identify any areas for improvement.

- It is important to deliver a dry run of the training to ensure that the content is sensitive to the needs of all participants.
- This is also an opportunity to identify learning techniques that might make the training more accessible for some groups: such techniques might include interpretation, closed captioning, the use of digital materials or the adaptation of visual settings. The dry run can be used to adapt and refine delivery.

6 Invite participants and circulate pre-training materials

Digital forensics and evidence training is often a core skill for law enforcement officers and members of the judiciary involved in combating cybercrime. It is essential to ensure that participants have the required level of preliminary knowledge to take the training.

Studies have shown that women tend to claim less knowledge than their counterparts, even though actual expertise is on par

Participants should be informed in advance whether they should complete any pre-training exercises or reading to help them prepare for the training. When delivering technical training on cybercrime issues, it is important to clearly explain technical concepts and processes: participants may find it helpful if a list of key definitions is circulated in advance of the training.

— Studies have shown that women tend to claim less knowledge than their counterparts, even though actual expertise is on par. Women may not have had sufficient opportunity to gain or operationalize some of their knowledge, especially in contexts where women, people with disabilities and other marginalized groups might not have had opportunities to engage in science, technology, engineering and mathematics (STEM) education. There may be opportunities to bridge gaps by circulating pre-training materials, starting with a compulsory introductory module, and/or by offering additional support and materials (e.g. stipends for further study) to participants.

7 Deliver the digital forensics training

The training may be delivered in several iterations or sessions. When delivering training to different participants via several iterations, it is important to ensure that the training is consistent to ensure that all participants acquire the same technical knowledge.

— The training should be consistent across sessions, but diverse learning techniques should be deployed as appropriate to meet the diversity of participants and their needs. This means recognizing, for instance, that some people may feel less comfortable than others in certain training environments; that both written and verbal contributions should be encouraged; and that participants should be encouraged to turn on their cameras in virtual training settings only if they wish to. It also means being open to, and prepared to make, reasonable accommodations for participation.

8 Handling comments and questions during the training

It is important to ensure that participants can offer comments and ask questions during the training. This can strengthen participants' understanding of the key issues addressed in the training.

— People understand and digest information in different ways. When delivering the training, anonymized comments or questions should be enabled. Where possible, trainers and organizers should make themselves available for follow-ups after the training concludes.

9 Assessment and accreditation

In some cases, completing the training will automatically result in accreditation, or will count towards an individual's continuing professional development. In other circumstances, participants may be required to successfully complete a technical assessment, based on the training, before gaining accreditation in a specific digital forensics skill. Consideration should be given as to whether resources are available to offer some form of accreditation.

- If women are accredited in the same way as their peers, they are more likely to get recognition for their technical skills and access opportunities for promotion.
- Accrediting participants might lead to opportunities which might otherwise be missed, and can also be used to encourage future cohorts to participate in the training.

Monitoring and evaluation

10 Enable post-training feedback

Participants should have the opportunity to provide post-training feedback, in particular to assess whether they have understood the technical concepts and processes addressed in the training.

- Feedback mechanisms will need to be appropriately developed to suit participants' needs. Enabling independent or third-party oversight of the training can help ensure impartiality. Allowing for the anonymous delivery of feedback will help overcome transparency barriers (e.g. self-censoring for fear of barriers to promotion).
- It is important to ensure that post-training feedback includes assessment of on-the-job applicability. People reflect on and operationalize learning in different ways: collecting feedback pertaining to this and disaggregating comments by gender allow for insights into how teachings are being received and used.

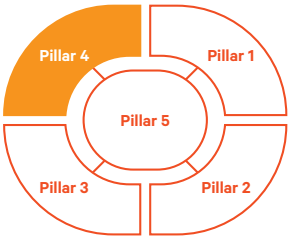
11 Analyse and assess the post-training feedback

After a period of six to 12 months, it is important to follow up with the participants who have completed the training to assess its impact. Insights from this follow-up process should be used as an opportunity to update, revise or otherwise improve the future development and delivery of the training.

- Including gender performance indicators (e.g. whether training reaches women and other marginalized people in meaningful ways or addresses learning barriers) in post-training feedback is a good way of assessing the different experiences of participants based on gender and other characteristics.
- With long-term projects, or extended periods of contact, it should be possible to assess the impact of training on real-life opportunities, like promotions or employment successes, or on developments in the field, such as policy impacts.

Pillar 4: Tasking and prioritization

This section discusses why gender is important when making operation decisions about resource allocation and prioritization in cybercrime response. An example project illustrates the steps involved in developing a reporting system for victims of cybercrime.



What do we mean by tasking and prioritization?

Tasking and prioritization explores how operational decisions are made about how resources are allocated, and how a balance is struck between pursuing strategic outcomes and responding to more immediate crime reporting. It focuses on which cybercrimes are prioritized with regard to response, investigation and prevention. This pillar also covers the mechanisms for setting the top-level operational priorities – including who decides which individual operations or investigations are prioritized and tasked, and how – as well as the sources, use and application of intelligence to inform priorities, and the operating procedures that are in place to support activities for combating cybercrime, such as crime reporting and victim support.

Projects that focus on tasking and prioritization include (but are not limited to):

- setting up reporting mechanisms or systems for cybercrime incidents;
- incident-response workshops;
- setting up a cybercrime database; and
- national and regional coordination on cybercrime.

Thinking about gender and tasking and prioritization

Gender is important for tasking and prioritization because it is only possible to tackle the **gendered impacts** of cybercrime if barriers to reporting, investigation

and prosecution are overcome. A study published by the Economist Intelligence Unit (2020) found that just one in four women who experienced online violence reported this to the platform(s) on which the violence occurred; only 14 per cent reported their experience to an offline protection agency.

Just one in four women who experienced online violence reported this to the platform(s) on which the violence occurred; only 14 per cent reported their experience to an offline protection agency

Different teams and agencies need to understand the drivers of vulnerability, whether these are violence- and/or abuse-related, and the gendered impacts of data breaches. Teams that are well equipped to understand how gender interacts with their area of work, and that can bring diverse voices into their governance, will be able to develop processes that reflect the needs of survivors and reduce the targeting of specific vulnerable groups.

In cases of online-perpetrated violence and abuse, reporting mechanisms should be informed by multi-stakeholder approaches and survivor-centric responses that relieve the reporting burden on the individual.

Key questions

Here are some key questions to consider when integrating gender in tasking and prioritization procedures:

- Which stakeholders should be engaged?
- What data and independent evidence need to be monitored and collected on the gendered dimensions of cybercrimes in order to ensure that systems are meeting needs?
- What measures are in place to ensure that the data are treated in a confidential and sensitive manner?

Example project: developing a reporting system for victims of cybercrime

This section uses an example project to demonstrate how gender can be integrated in tasking and prioritization. The example given considers the development of a reporting system for victims of cybercrime.

Planning

1 **Set the stage for the cybercrime reporting systems, consult stakeholders and define the scope**

The relevant strategic objectives of the cybercrime reporting system for victims must be identified at the outset. It is useful to understand how these form part of any existing overarching national cyber strategy and national cybercrime action plans.

The reporting of data on victims of cybercrime can be abused by various people and organizations who are tasked with managing it, leading to serious violations of privacy. Government departments and civil society groups should be aware

of what data can and should be collected, and how and when data should be processed and published.

Cybercrimes are under-reported. Data and evidence already exist on offline gender-based crimes, and these can help inform a reporting system for online gender-based harms

Once the data management process has been established, it is essential to identify which types of cybercrimes can be reported and how they will be reported. It is also important to be able to direct users to helplines or other methods of reporting for crimes not covered by the reporting system.

- Cybercrimes are under-reported. Data and evidence already exist on offline gender-based crimes, and these can help inform a reporting system for online gender-based harms.
- Stakeholders should be involved from the initial stages of establishing strategic goals. Strategic objectives should be developed in consultation with key stakeholders representing women and other marginalized groups. These organizations should be able to report on behalf of a survivor to avoid the additional burden associated with reporting. Additionally, these stakeholders – especially those working in victim support – should help define the scope of the victim reporting, including (among other things) what types of crimes are covered.
- Key questions to consider include the legal parameters under which the reporting system operates, the exemptions the cybercrime reporting system's employees would need in order to conduct their work, issues relating to data storage, the reporting system's legal liabilities, and its registered status (for example, whether it is a charity).

2 Secure sufficient budget and resources

For the cybercrime reporting system to be successful, planning and allocating appropriate resources – including a dedicated budget and project staff – is vital.

- A cybercrime reporting system for victims that meets the needs of the diverse population is likely to involve multiple actors. Reporting systems must be accessible for people living in rural locations and for marginalized groups.
- As such, no one agency can be responsible for the system; responsibility should be shared across agencies. It is important to decentralize funding to increase reach, scope and accessibility.
- Reporting systems may also be embedded in other policy areas or in ministerial departments, for example within the ministries of education, healthcare, finance or business. This in turn will promote the efficacy and visibility of reporting systems, including making these more sustainable due to higher levels of buy-in and responsibility.

3 Identify who will manage the cybercrime reporting system

Crimes are usually reported to a national phone line or to individual police forces. Therefore, as regards cybercrimes, it is important to establish which authority will be responsible for managing the reporting system, and whether this will be managed nationally or locally.

— To alleviate the burden of reporting on the survivor, there should be multiple ways of accessing or using a cybercrime reporting system.

— A board or commission might be an appropriate lead for managing a cybercrime reporting system, as many law enforcement agencies are not appropriately sensitized to receive reports of this nature. In countries where social norms might mean that police forces are not sufficiently independent to handle such sensitive reports, an intermediary might be considered, such as a national human rights institution, a women's rights commission or an NGO.

4 Decide who will develop the cybercrime reporting system

Some authorities or agencies may have the capacity to develop a cybercrime reporting system in-house. However, development can also be contracted out to a third party. It is important that the developer is aware of any policing and victim reporting principles that are already in place, as well as any data protection obligations.

— In many countries, data protection legislation is not robust and often fails to regulate and manage information in a manner that prioritizes the protection of the individual. In contexts where there are limited regulations, it is advisable to engage a UN agency or an NGO to assist in establishing such mechanisms.

— It is important to be mindful of local political, social and cultural norms and contexts that might compromise basic requirements of gender-sensitive reporting. For example, are women and other marginalized groups involved in developing the reporting system? What datasets are being used, and how is testing being conducted? Is the reporting system designed in an accessible format? If the reporting system is online, can it be accessed where bandwidths are low?

Implementation

5 Develop the system, and train the staff and team

When developing the reporting system, training the team, stakeholders and staff who will be involved in its delivery is essential. This includes sharing best – including sensitive – practice in delivery and cooperation, and ensuring a good understanding of the relevant laws, regulations and frameworks.

— The needs of law enforcement must be balanced with developing an effective system that works for those who are affected by cybercrimes. Internal communication and liaison will be important, as will ensuring the safe sharing of information. Institutional policies on information protection should be in place throughout an agency or department. The exact protocol for what information is needed should be developed following universal guidelines.

— The reporting of cybercrimes that impact gendered groups differently is often vulnerable to bias. The handling of these crimes can similarly be subject to bias. It is essential to train staff and teams to address bias, and to ensure the inclusive delivery of operations. A **safeguarding** approach is key to ensuring sensitive implementation. Staff working on reporting (e.g. the receipt of cases) should

have different profiles to operational staff – although there should be diversity in terms of expertise and background among staff handling reports, as well as among staff handling operational aspects.

6 Develop a communications plan

A communications plan can help to successfully launch the system and raise awareness of its purpose and the potential impacts. This plan should seek to raise awareness among government agencies and law enforcement, civil society, industry and the public.

- The design and implementation of a communications plan should be closely aligned. The plan must show understanding of the dynamics around vulnerabilities, reporting barriers and the way information is consumed among people who are harder to reach.
- It is important to partner with relevant actors (trusted by the community) to communicate with segments of the intended audience.
- Key principles for communication include: ensuring feedback loops to understand if communications are appropriate; avoiding stereotypes; addressing fear of retaliation; raising awareness around harms; tackling social norms and stigmas; and explaining the safeguards that are in place.

7 Launch the system

The launch of a system should begin with a 'start-up' period that is appropriate to the length of the project or funding cycle (i.e. a start-up period of a couple of months would suffice for a shorter project). During this period, capacity-builders should ensure that learning around gender and inclusion is meaningfully actioned in adaptation. There are two key stages in doing this. Within these two stages, there are several important steps to consider:

- The first of these stages is the troubleshooting of issues with the system. This focuses specifically on monitoring the system during the immediate period after launch.
  - Ensuring access at both ends of the system (for both reporters and call handlers) requires logistics. Some individuals may not have access to reporting systems, despite investment and planning. It is essential to continue regular meetings with civil society (especially in rural areas) to address gaps in reach, and to understand what additional resources may be needed.
  - Staff may require additional training, and should have regular mentoring to address problematic reports or issues they are unfamiliar with. Using budget allocated to increase staff capacity, these issues can be addressed with the help of external and trusted expertise. Additionally, staff should have access to specialist psychological and related services to support their well-being.
  - Regular liaison with offline partners such as police, lawyers and community leaders will be essential to ensure responsiveness to crimes and to establish efficient working relationships.

It is essential to continue regular meetings with civil society (especially in rural areas) to address gaps in reach, and to understand what additional resources may be needed

- In terms of acquisition of evidence, social media companies and **internet service providers** are essential to reporting and evidence protocols. Requesting a point of contact in these organizations will help ensure effective troubleshooting and cooperation in the start-up phase.
- The cybersecurity of the reporting system should never be an add-on. Data protection protocols and encrypted security should be constantly addressed, whatever software is used in the system.

- The second stage is feedback and adaptation. This involves the continuous updating of the system to ensure that key performance indicators (KPIs) are met and that learning from the first stage is implemented.
  - Having an on- and offline feedback loop that allows users to anonymously provide feedback on experiences of reporting can be valuable. Adjustments should be made in line with feedback to improve reporting experiences.
  - When looking at data, it is important to try to assess which groups are still excluded. Comparative data on the responsiveness of reporting mechanisms, disaggregated by gender, age and other demographics, can help shed light on this area.
  - Ultimately, referrals and the outcomes of cases should be informed and designed by survivors. This can be done in coordination with relevant stakeholders, but survivor-led and survivor-friendly recourses must be prioritized.
  - Where there are gaps in data (such as in third-party evidence from hosting providers), KPIs should be developed (if resources allow) specifically to enable those gaps to be filled. Working with a third-party monitor can help provide in-depth assessment of whether KPIs and adaptation have delivered in terms of gender and inclusion needs, and whether the reporting system has met the targets as originally set.

Having an on- and offline feedback loop that allows users to anonymously provide feedback on experiences of reporting can be valuable

Monitoring and evaluation

8 **Collect and analyse reporting data, and review the cybercrime reporting system**

Periodically analyse reporting data and share insights with key stakeholders, both within law enforcement and elsewhere.

After 12 months, the data gathered from the reports and user feedback should be reviewed. Doing this will help to measure impact and progress towards objectives. This is also an opportunity to make sure that the cybercrime reporting system remains up to date, taking account of the evolving nature of cybercrimes.

- It is important to share anonymized evidence and learning, and to bring in offline actors to review reporting systems and revise them as necessary. Relevant KPIs could include:
  - reporting data that has been disaggregated, e.g. by gender, age or location;
  - response times;
  - complaints addressed and responded to; and
  - identification of perpetrators of other crimes.

- This anonymized data collection can then inform proactive activities such as the development of educational workshops on gendered cybercrimes to help raise awareness of harms, and of how victims can seek support; or the formation of victim support hubs with supplementary support mechanisms.
- Where various agencies have authority over the reporting system, data collection and formatting should be standardized. This makes analysis easier and ensures continuity in ongoing evaluation.

Glossary

The definitions in this glossary are drawn from several sources, including Chatham House's resource *Gender, think-tanks and international affairs: a toolkit* (2021); Stonewall UK; the European Institute for Gender Equality; and UN Women. The definitions in this glossary are non-exhaustive, and every effort has been made to sure they are accurate, representative and inclusive.

Cybercrime
There is no strict or universal definition of cybercrime, but the term is often used to refer to criminal activities carried out on or using the internet.

Cybercrime capacity-building
Cybercrime capacity-building describes the work of experts and national, regional and international organizations in developing, implementing and strengthening measures for responding to, reducing and combating cybercrime.

Cyber-dependent crimes
Cyber-dependent crimes are crimes that are committed using ICTs.

Cyber-enabled crimes
Cyber-enabled crimes are crimes that are carried out online but may also be committed offline.

Do no harm
Under 'do no harm' principles, an action is conducted in a way that avoids exposing already vulnerable people to additional risks and harms. This is done by actively seeking to mitigate negative impacts and designing interventions accordingly.

Gender
Gender refers to structural and cultural systems and markers that are often expressed in binary terms of masculinity and femininity. Gender exists on a spectrum and is socioculturally constructed. The word 'gender' is also often incorrectly assumed to be synonymous with 'women'.

Gender-aware
Being gender-aware means being cognizant of the gendered impacts of an activity, policy, position, product, etc., and actively working to mitigate or reduce harms from such impacts.

Gender-blind
Being gender-blind is to not consider someone's gender when making a decision.

Gender-disaggregated
Gender-disaggregated often refers to data, but can also relate to other aspects of analysis. To gender-disaggregate something is to collect and tabulate information based on gender identity to ensure the acknowledgment and analysis of differences.

Gender equity and sensitivity
Gender equity and sensitivity refers to fairness in the treatment of people, with appropriate accommodations made for those who are historically disadvantaged or marginalized, and awareness of the inherent biases and stereotypes that manifest themselves as discrimination. When activities, policies and processes are 'gender-sensitive', it means that they intentionally treat people as equal and with respect, and address inequalities that derive from gender identity.

Gendered harms
Gendered harms refer to risks, harms and discrimination of and to a person based on – and often specific or exclusive to – their gender. These are not always sexual harms or sex crimes.

Gendered impacts
Gendered impacts refer to the likely outcomes or consequences of an activity, policy, position, product, etc. based on an individual's gender identity. These are often negative consequences, or consequences that reinforce cultural hierarchies.

Gender lens
Applying a gender lens to something means actively assessing its gendered impacts.

Gender-neutral
Gender-neutral refers to scenarios, products, innovations, etc. that have neither a positive nor a negative impact when it comes to gender relations.

Gender-nonconforming
A person who is gender-nonconforming does not align with the conventional traits attributed to any gender.

Gender-responsiveness
Gender-responsiveness means that intended and realized outcomes have reflected on gendered inequalities.

Internet service provider
An internet service provider (ISP) is a company that provides users with access to the internet.

Interpersonal crime
Interpersonal crimes are ones that are often committed repeatedly in order to establish a pattern of behaviour that uses fear or intimidation to exert control over another person.

Intersecting identities
The study of intersectionality, a term coined by Kimberlé Crenshaw, seeks to understand how gender interacts with race and other social categories and identities, and how forms of discrimination are manifested based on these intersections. Intersecting identities refers to the multiple categories and

characteristics with which people identify. Often these identities are perceived as being inseparable.

Male-by-default design
Male-by-default design refers to the concept that the default gender – among and for which systems, concepts, ideas, policies and activities have been designed – is 'man'. This is related to androcentrism, which is the practice of centring a masculine world view and marginalizing others.

Non-binary
Non-binary refers to people who do not identify as 'man' or 'woman'. This can also include people who identify with some aspects of the identities that are traditionally associated with men and women.

Safeguarding
Safeguarding is the act, process or practice of protecting people from harm, and the measures in place to enable this protection.

Resources

Gender, cyber and international security

Gender Approaches to Cybersecurity, UNIDIR, 2021
This report explores how gender norms shape specific activities pertaining to cybersecurity design, defence and response: https://unidir.org/publication/gender-approaches-cybersecurity

Why Gender Matters in International Cyber Security, WILPF and APC, 2020
The report identifies multiple gender-differentiated impacts of cyber operations with an international dimension, such as internet shutdowns, data breaches and disinformation campaigns, and builds the case that these differentiated impacts need to be better accounted for and understood by policy-making and technical communities: https://www.reachingcriticalwill.org/resources/publications-and-research/publications/14677-why-gender-matters-in-international-cyber-security

System Update: Towards a Women, Peace and Cybersecurity Agenda, UNIDIR, 2021
This paper analyses the linkages between WPS priority themes – gender equality, women's participation in international security, prevention and protection of violence against women, gender-differentiated needs – and international cybersecurity. It identifies priority areas that should be addressed to ensure a gender-inclusive cyberspace that protects the rights of women and girls: https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

Gender equality, cybersecurity, and security sector governance, 2022
This paper explores the link between good governance in cybersecurity and gender equality, setting out how an approach to cybersecurity that focuses on principles of good governance can help ensure gender equality: https://www.dcaf.ch/gender-equality-cybersecurity-and-security-sector-governance

Gender mainstreaming and gender strategies

Strategy for Gender Equality and the Empowerment of Women (2018–2021), UNOV/UNODC
This strategy seeks to ensure that gender equality and the empowerment of women and girls are integral parts of all aspects of work of UNOV/UNODC in making the world safer from drugs, crime and terrorism and in ensuring the peaceful uses of outer space: https://www.unodc.org/unodc/en/gender/the-gender-strategy.html

Women in Law Enforcement in the ASEAN Region, Interpol, UNODC and UN Women, 2020

This report explores the experiences and views of women police officers from across the ASEAN region and provides a snapshot of current practices for their recruitment, training, deployment and promotion: https://www.interpol.int/en/News-and-Events/News/2020/Women-increase-operational-effectiveness-of-policing-but-barriers-persist-ASEAN-report

Gender and Strategic Communications in Conflict and Stabilisation Contexts, UK Government, 2020

This guide instructs users on producing gender-sensitive strategic communications in conflict and stabilization contexts: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866351/How_to_Guide_on_Gender_and_Strategic_Communication_in_Conflict_and_Stabilisation_Contexts_-_January_2020_-_Stabilisation_Unit.pdf

The Women's Empowerment Principles Gender Gap Analysis Tool

The Women's Empowerment Principles (WEPs) Tool is a business-driven tool designed to help companies from around the world assess gender equality performance across the workplace, marketplace and community: https://weps-gapanalysis.org

Gender Mainstreaming, European Institute for Gender Equality

This toolkit helps users integrate a gender perspective into all stages of policymaking and strategic planning: https://eige.europa.eu/gender-mainstreaming

Gender Based Analysis Plus (GBA+), Women and Gender Equality Canada

GBA+ is an analytical process that provides a rigorous method for the assessment of systemic inequalities, as well as a means to assess how diverse groups of women, men and gender-diverse people may experience policies, programmes and initiatives: https://women-gender-equality.canada.ca/en/gender-based-analysis-plus/what-gender-based-analysis-plus.html

Integrating Gender Into Internal Police Oversight, DCAF, 2014

This guidance note is a resource for police services. It covers providing equal opportunities, monitoring different security needs based on gender, and ensuring gender sensitivity is embedded in all internal systems and processes: https://www.dcaf.ch/integrating-gender-internal-police-oversight

Gender-based violence (GBV) online

University Teaching Module on gender-based interpersonal cybercrime, UNODC

This module is designed to teach participants how to define interpersonal cybercrimes, differentiate between them, analyse the ways in which ICTs are used to facilitate these crimes, and identify the challenges to reporting and preventing

these cybercrimes: https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html

Report of the UN Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, UN Human Rights Council, 2018
This is a report of the UN Special Rapporteur on violence against women and girls which covers online violence. The report considers how violence against women has been facilitated by new technologies and digital spaces from a human rights perspective: https://undocs.org/A/HRC/38/47

Gender mainstreaming in thematic areas: Gender equality and cybercrime/ cyberviolence, Council of Europe
This factsheet outlines the Council of Europe's approach to gender equality in cybercrime/cyber violence: https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cybercrime-cybervi/168092e9b4

Measuring the prevalence of online violence against women, Economist Intelligence Unit, 2020
A study aiming to develop a credible and granular measurement of the global prevalence of online violence against women: https://onlineviolencewomen.eiu.com

Report of the National Dialogue on Gender-based Cyber Violence, IT for Change and Advanced Centre for Women's Studies, Tata Institute of Social Sciences, 2018
This is the report on a two-day national dialogue on gender-based cyber violence, which took place in Mumbai, India, in 2018. The dialogue aimed to facilitate a systematic stocktaking of the phenomenon from a gender equality perspective: https://itforchange.net/e-vaw/wp-content/uploads/2018/03/Event-Report-of-National-Dialogue-on-Gender-Based-Cyber-Violence.pdf

Online Gender-based Violence in the Philippines, Foundation for Media Alternatives, 2021
This report looks at how online gender-based violence in the Philippines has developed: https://fma.ph/2021/02/19/online-gender-based-violence-in-the-philippines-our-year-end-round-up-report

Women and cyber crime in Kenya, Global Information Society Watch, 2013
This report on women and cybercrime in Kenya provides an overview of anti-cybercrime policy and legislation in the country: https://giswatch.org/en/country-report/womens-rights-gender/kenya

Cyber Harassment Helpline Report, Digital Rights Foundation, 2020
This is an annual report on the Cyber Harassment Helpline managed by the Pakistan-based NGO Digital Rights Foundation. The report includes the journey of the development of the helpline, and provides facts and figures on the number

of cases reported to the helpline in 2020: https://digitalrightsfoundation.pk/wp-content/uploads/2021/02/Helpline-Report-2020.pdf

Online and ICT-facilitated violence against women and girls during COVID-19, UN Women, 2020
This briefing paper focuses on the emerging trends and impacts of COVID-19 on ICT-facilitated violence against women and girls, and provides examples of strategies and practices put in place to prevent and respond to such online and ICT-facilitated violence: https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19

How to Store Data, Take Back the Tech!
This 'how-to' guide provides technical advice and tips on how to store data related to incidents of violence against women and girls: https://takebackthetech.net/be-safe/how-store-data

Handbook for the Judiciary on Effective Criminal Justice Responses to Gender-based Violence against Women and Girls, UNODC, 2019
This handbook aims to raise awareness of, and foster use and application of, the relevant international standards and norms by the judiciary when dealing with criminal cases involving gender-based violence against women and girls: https://www.unodc.org/pdf/criminal_justice/HB_for_the_Judiciary_on_Effective_Criminal_Justice_Women_and_Girls_E_ebook.pdf

Cyber Violence against Women and Girls: A world-wide wake-up call, UN Broadband Commission for Digital Development, 2015
This discussion paper draws attention to emerging trends and intends to start discussions on the implications of these trends on efforts to advance gender equality and the empowerment of women in the digital age. This paper recognizes the wide range of issues related to cyber violence, and does not present itself as a full compilation of those issues or of proposed solutions: https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

Design ethics for gender-based violence and safety technologies, Oxford Internet Institute, 2017
This workshop, held in 2017 at Princeton University, explored the design ethics of gender-based violence and safety technologies: https://www.oii.ox.ac.uk/blog/design-ethics-for-gender-based-violence-and-safety-technologies

Mapping research in gender and digital technology, APC, 2018
This report considers the gender biases and stereotypes that are embedded in technology, and how these reproduce the existing problems around gender parity, gender-based violence, discrimination and exclusion on the internet: https://www.apc.org/en/pubs/executive-summary-mapping-research-gender-and-digital-technology

Cyber Violence against Women And Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach, DCAF, 2021
This report uses case studies to focus on gendered violence online in the Western Balkans. It presents cyber violence from the perspective of cybersecurity governance. The case studies refer to the relevant national legal and governance frameworks. The report identifies governance gaps and provides recommendations: https://www.dcaf.ch/cyber-violence-against-women-and-girls-western-balkans-selected-case-studies-and-cybersecurity

Human rights and technology

Introduction – human rights and equity in cyberspace, Robin Mansell via LSE Research Online, 2004
This chapter provides an overview of the key debates on human rights and equity in cyberspace: http://eprints.lse.ac.uk/3707/1/Introduction%E2%80%93Human_Rights_and_Equity_in_Cyberspace_%28LSERO%29.pdf

Internet Rights Are Human Rights, training curriculum, APC, 2021
This training curriculum, produced by the Association of Progressive Communications, is concerned with the interface between human rights, ICTs and the internet, including the relationship between the international human rights regime and communication rights: https://www.apc.org/en/pubs/internet-rights-are-human-rights-training-curriculum

Cybersecurity and Human Rights, GCCS2015 webinar series, Global Partners Digital, 2015
This workshop summary provides an introduction to cybersecurity, with a particular focus on the policy aspect of cybersecurity, including how cybersecurity is addressed in international relations and the impact cybersecurity has on human rights: https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf

Cybersecurity and Human Rights, webinar presentations, Council of Europe, 2020
This series of presentations from a Council of Europe webinar on cybersecurity and human rights held in December 2020 captures the key issues on the current state of human rights safeguards and guarantees applicable to state policies, regulations and measures to ensure security of cyberspace, against the backdrop of the COVID-19 pandemic: https://www.coe.int/en/web/cybercrime/cybersecurity-and-human-rights

University Teaching Module on international human rights and cybercrime law, UNODC
This module examines the legal landscape relating to cybercrime, highlighting the need for harmonized legislation and outlining the relationship between cybercrime laws and human rights: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html

About the authors

Rebecca Emerson-Keeler is the gender and inclusion consultant on the Chatham House project on building anti-cybercrime capacity in Southeast Asia. She has over 15 years' experience in researching, managing and evaluating programmes in conflict and fragile states; assessing and designing conflict and gender-sensitive interventions; building capability of MENA institutions and governments; and working with commercial actors, governments, the UN and civil society on migration, strategic communications, preventing and countering violent extremism, and gender.

Amrit Swali is a research associate in Chatham House's International Security Programme and part of the editorial team of the institute's *Journal of Cyber Policy*. Amrit is also the co-chair for gender on Chatham House's Equality, Diversity and Inclusion Working Group. Amrit's research work focuses on cybercrime policies, international cyber governance and the intersection between gender, international security and cyber.

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

Esther Naylor is a former research analyst in the International Security Programme at Chatham House. Her expertise sits at the intersection of geopolitics and technology. At Chatham House, Esther delivered cybersecurity capacity-building exercises for government officials, produced analysis and multimedia campaigns on cyber governance and international cyber diplomacy, and researched gender and cybercrime. As a member of the editorial team of the *Journal of Cyber Policy*, she contributed to the development of special issues on topics including internet consolidation and inclusive cyberspace governance.

Esther holds an MA in security and international law from the University of Manchester, and a bachelor's degree in international relations and French from the University of Birmingham.

Acknowledgments

This toolkit was produced as part of a project funded by Global Affairs Canada.

The authors would like to thank Joyce Hakmeh, James Shires, Jamie Saunders, Robert Collett, Isabella Wilkinson and Emma Saunders for their individual and collective expertise and guidance on the toolkit's content and structure. They also thank the members of the project's advisory group for their advice, insights and recommendations. Finally, the authors thank Jo Maher, Vera Chapman Browne and the Chatham House publications and digital transformation teams for their support.

ISBN 978 1 78413 551 5
DOI 10.55317/9781784135515

Cite this publication: 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.

designbysoapbox.com

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, helps governments and societies build a sustainably secure, prosperous and just world.

Chatham House is an independent policy institute and a trusted forum for debate and dialogue. Our research and ideas help people understand our changing world. Chatham House events offer unique access to thought leadership, best practice and insight from world leaders, policy influencers and academics. We deliver webinars, conferences and simulations that help connect diverse, engaged audiences and build momentum for positive change.

Contact

internationalsecurity@chathamhouse.org
www.chathamhouse.org