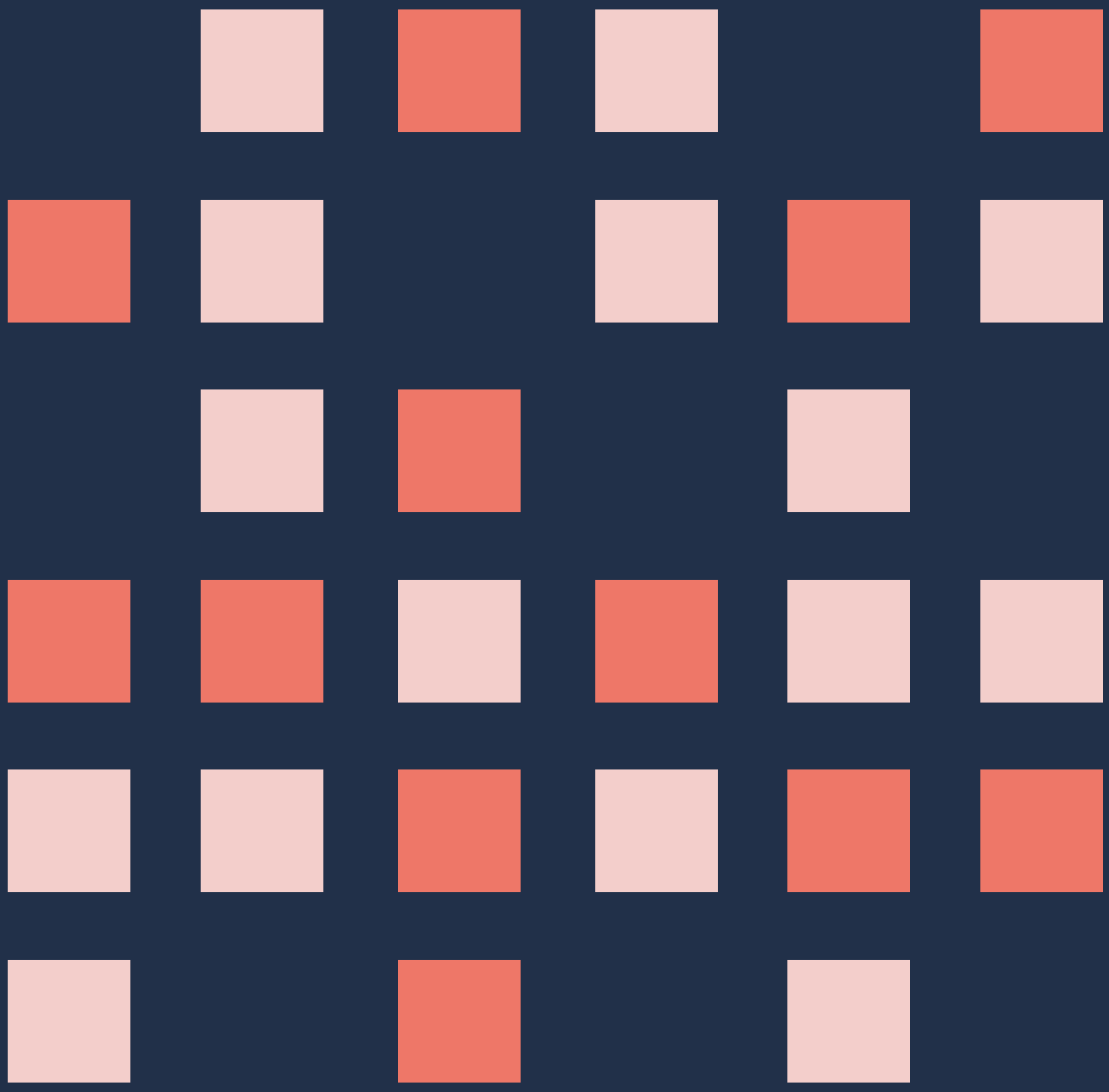
Inclusive Cyber Norms

Toolkit



GLOBAL PARTNERS DIGITAL

2023

Acknowledgments

This toolkit was developed and drafted by Global Partners Digital. Its development would not have been possible without the following individuals, who contributed their expertise to its development and drafting:

- Veronica Ferrari, Association for Progressive Communications (APC)
- Dr Katharine M Millar, Department of International Relations at the London School of Economics
- Allison Pytlak, Stimson Centre (former WILPF)
- Dr Tatiana Tropina, Institute of Security and Global Affairs at Leiden University

We would also like to express our gratitude to the following individuals, who were consulted by Veronica Ferrari as part of its development:

- Adeboye Adegoke, Paradigm Initiative
- Vivian Affoah, Media Foundation for West Africa
- Enrico Calandro, Cyber Resilience for Development (Cyber4Dev)
- Lillian Nalwoga, Collaboration on International ICT Policy in East and Southern Africa(CIPESA).

Finally, we owe a debt of thanks to Isabel Lecaros for their work on the design of the toolkit, and to Ana Pleite for its translation into Spanish.

The development of this toolkit was made possible with support from Global Affairs Canada.

Table of contents

Foreword

Why we created the toolkit

The aim of cybernorms is to create a peaceful and secure cyberspace, by shaping the way actors behave, and how threats are addressed.

But cyberspace is not experienced equally by everyone. Marginalised stakeholders—including women, LGBT+ communities, racialised groups, people in the Global South, and those in vulnerable professions (e.g activists and security researchers)—face elevated and particular risks in the digital environment: from harassment and stalking to state-sponsored hacking. They may also face specific obstacles to exercising their human rights in cyberspace—ranging from economic constraints to language barriers and access gaps.

Despite this, cybernorm processes currently pay little heed to including marginalised stakeholders. They are underrepresented and under consulted. Even when factors like gender, race and sexuality are technically considered, it is often in a cursory or non-nuanced way. As a result, the implementation of cybernorms not only fails to adequately speak to the experiences of marginalised communities—it can even serve to diminish it.

The solution to this state of play? A rigorously inclusive approach to developing and implementing cybernorms. That is what this toolkit aims to promote and facilitate.

Built on extensive research and consultation with a range of stakeholders and experts engaged in ongoing cybernorm processes—including the UN's Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG)—it offers tailored and concrete guidance on considering inclusivity in norm development and implementation through policymaking processes, including:

- → An introduction to key terms and concepts relevant to inclusivity and cybernorms;
- → A how-to guide on fostering an inclusive process for developing cybernorms or implementing existing norms;
- → A supplementary set of practical resources to support the implementation of inclusive policymaking processes.

Tool 1	How to facilitate inclusive stakeholder mapping processes
Tool 2	An explainer on understanding inclusion terminology
Tool 3	An explainer which maps regional and global cybernorms processes

In this section, we'll set out what you need to know about cybernorms, and the rationale for an inclusive approach.

Section 1

Why should the development and implementation of cybernorms be inclusive?

What is a cybernorm?

A norm refers to a common understanding of what constitutes appropriate behaviour for actors within a particular community.

Cybernorms, therefore, broadly refer to shared ideas about how actors (e.g states, private corporations, civil society organisations, and individuals) are expected to act in cyberspace, with respect to the use of digital technologies.

They can take a range of forms. They may be shared ideas (like the general consensus that human rights must be respected online), and may include written, voluntary and non-binding commitments, agreements, policy frameworks, or statements of principle. Examples include the **eleven United Nations Group of Governmental Experts (GGE) norms, ASEAN Data Management Framework**, and the **Tallinn Manual**.

A key focus of cybernorms is limiting and tackling cyber threats, which can also take a variety of forms—from large state-sponsored cyber attacks, to hacking, harassment, and stalking. Cybernorms can also have a positive dimension, in setting out mechanisms for capacity building, protection and promotion of rights-respecting policies and cooperation. To have an impact, these commitments are usually translated and implemented through the development of national or regional policies and regulatory frameworks, such as cybersecurity strategies, issue-specific cybersecurity policies, and regulation.

What is an approach inclusive of marginalised communities?

Inclusive approaches to policymaking are premised on the idea that including relevant stakeholders in a process has both an intrinsic and a practical value: as we set out in **our guide for inclusive policymaking**. That is to say: it is ethically right, reflective of both human rights and democratic principles, while also resulting in policies that are more effective and impactful.

Generally speaking, an inclusive approach to cyber policymaking seeks to meaningfully include:

1. Those with a mandate, role, or responsibility in the process
2. Those with skills or expertise needed to inform the policy and operationalise it;
3. Those who could be disproportionately affected by the policy or its implementation—i.e. marginalised groups

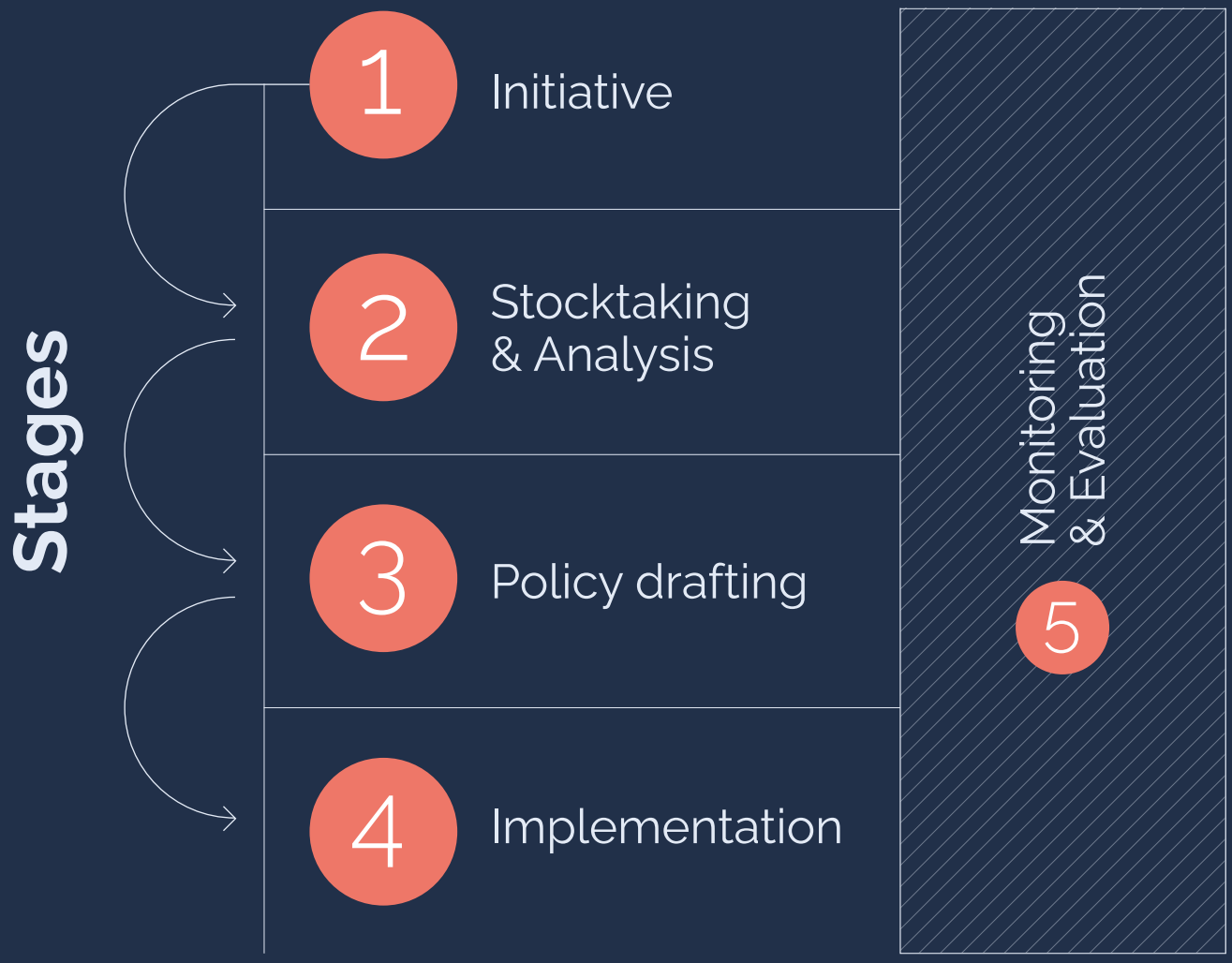
In this toolkit, we focus particularly on that third group (though of course, they all overlap), with the aim of setting out the particular considerations, sensitivities and adjustments which should be taken into account to ensure that marginalised groups are able to meaningfully participate.

The resources below—including a step-by-step guide to including marginalised groups at each policy stage, as well as tools for specific tasks and components—offer guidance that is both concrete and granular. But they are also anchored in broad principles, which any truly inclusive process must embody: being open and accessible to different types of input; a focus on fostering consensus, through mutual understanding and trust; and clear, transparent communication about the process and its outcomes.

In this section, we set out a five-stage process to ensure cybernorm policy processes and outcomes are developed inclusively.

Section 2

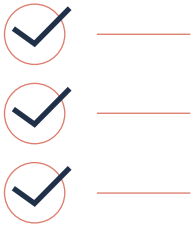
How to make cybernorm policymaking processes inclusive of marginalised perspectives and stakeholders



Stage 1 Initiative

This is the preparatory stage of any policymaking process—where policymakers work to secure political buy-in, finalise the strategic vision of the policy, establish key structures and processes, and identify relevant stakeholders. At this stage, marginalised perspectives should be involved in a clear and accountable process, agreed with stakeholders, to advise policymakers and make decisions on an equal footing. The key here is transparency and clear lines of communication.

Things to do at this stage



- **Conduct an inclusive stakeholder mapping** to determine which communities you need to hear from and engage with in your process. A good mapping should identify marginalised groups who may be particularly impacted by cyber threats, as well as ways to account for and overcome potential obstacles to their participation. See Tool 1 for detailed guidance on how to achieve this.
- **Proactively put in place measures to enable participation of marginalised groups/individuals**. This might include, but is not limited to:
  - **Posting deadlines well in advance** for registering interest in participation and consultation.
  - **Accepting inputs in non-written formats** (e.g. oral testimonies, videos, photographs, biographical narratives, or structured conversations).
  - **Allocating funding and material resources** to people and groups to enable them to participate, including funding for ICT connectivity, for travel, for accommodation and subsistence, for child and eldercare.
  - **Translating materials** from both policy development process and formal global and regional cybernorm processes into all stakeholders' preferred languages. Similarly, all multistakeholder inputs and submissions should be translated into all the official languages of a specific organisation. For example, to ensure multistakeholder contribution to global ICT and cybernorm governance consultations in the UN, the materials should be translated into 5 UN languages.
  - Develop careful procedures and guidelines, in consultation with stakeholders, for ensuring privacy and safeguarding for all involved in the policy development process through holding closed door meetings, observing Chatham House rules or providing safe and secure ways to provide input (e.g. anoynmous contributions or through encrypted channels).
- **Establish clear lines of communication and reporting so everyone is kept up to date with progress**. This will support the transparency and accountability of the process. Ongoing participation may also involve agreement as to how complaints, disputes, and disagreements throughout the process will be addressed (this might include substantive policy differences, but also instances of unmet commitments, or experiences of discrimination or marginalisation, within the policy development process).

Extra considerations

- Consult with identified stakeholders to find out what form (if any) of **capacity building and training** they would find helpful and productive (while also being mindful that such training can also reproduce patterns of discrimination).
- Cultivate **reflexivity**. Carefully think through your own social positioning, preconceived notions, potential biases, and relationship to existing forms of power and privilege, to evaluate how that might be informing decision-making at this stage.
- Be attentive to **existing hierarchies and dynamics** between stakeholders across and within sectors (e.g. civil society and the private sector). It is important to always amplify and accommodate input from groups typically excluded or sidelined from cybernorm processes.
- Establish a model and budget for **compensating people for their time and expertise** in multistakeholder consultations and participations. This will help ensure processes are collaborative, rather than extractive.

Success might look like:

→ A comprehensive stakeholder mapping, which has been agreed by actors leading the process;
→ Established contact with a broad range of stakeholders from different marginalised groups;
→ A shared understanding of what it means for the policy development process to be open, as well as potential barriers to participation;
→ Identification of proactive measures to overcome these barriers.

Stage 2 Stocktaking & Analysis

With the relevant stakeholders identified, this stage focuses on determining where their input would be particularly useful—through a survey and close analysis of the existing policy landscape.

Things to do at this stage

- **Engage in ongoing dialogue with identified groups to understand their experiences and perspectives.** This is important for the transparency and accountability of the process. It will take time and be an iterative process of exchange and two-way information-sharing about how input is being considered or integrated. It cannot be treated as a box-ticking exercise. Individuals participating in these dialogues should consider how their identities may influence the willingness and trust of participants to share information.
- **Develop a shared understanding of how gendered and marginalised groups are affected by cybernorms and, particularly, cyber threats**—with input from marginalised groups as identified in the mapping. This might take the form of a reference document or concept note, which outlines and maps discriminatory impacts—including gendered and racialised impacts—of the identified cyber threats within specific contexts. It might also include a close legal analysis of the policy in question through this identity-based framing, to identify any specific, concrete risks.
- **Be proactive in getting input from stakeholders**. Don't assume that issuing a general call for input is enough. Instead, reach out directly to marginalised groups that you've identified in your stakeholder mapping, taking their capacity and experience of engagement into account. This is especially important when soliciting input from groups who are exposed to significant forms of disadvantage, and who may lack access to conventional organisational structures or pre-existing institutions.
- **Report back and maintain relationships with the stakeholders that have been consulted with to share the results of the analysis**. Make sure the document/s are accessible and take into account different needs. Let stakeholders know how the policy process is unfolding, if and how their points are being addressed, and give them the chance to input on draft documents.

Extra considerations

- Reflect carefully about how gendered, colonial, and racialised ideas inform the knowledge-creation process within policy development. Established standards of knowledge—and forms of academic and institutional language—can shape what kinds of stakeholders are seen as "credible".

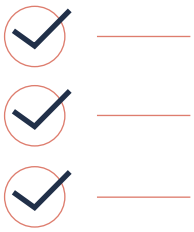
Success might look like:

→ Stakeholders are substantively engaged in conversations, and express that they are comfortable and happy with their level of inclusion;
→ There is a shared understanding of how gendered and marginalised groups are affected by cybernorms.

Stage 3 Policy drafting

This stage focuses on the development of the text itself. Stakeholders should be engaged at all points in the production process, but particularly in reviewing and commenting on draft versions of the text.

Things to do at this stage



- Ensure that **identified stakeholders are included** in the drafting process and that the measures put in place under Stage 1 remain appropriate.
- **Publish stakeholder inputs into the process.** These should be in a format that is easily accessible to all stakeholders. Ensure that stakeholders are fairly acknowledged and credited for their contributions.
- Use **accessible language** and ensure that you account for differences in level of language and familiarity with certain registers (e.g. some participants may not be as sensitised to academic modes of expression). This is important for openness and accessibility. For example, if oral input is necessary, ensure that this is transcribed accurately; and allocate funds and time for translation, especially if you are trying to reach marginalised communities who use different local dialects and languages.
- For transparency, ensure that **all draft text takes into consideration the findings and expertise** from Stage 2, checking in regularly to consider potential impacts and harms from language and wording on marginalised groups. Communicate the timeline and modalities of the drafting stage to stakeholders, ensuring there is adequate time to review text and input.
- Build in **regularly scheduled updates and points of participation and input**, throughout the drafting stage for all consulted stakeholders and key actors, to make sure feedback and drafting is an iterative process.

Extra considerations

- Consensus is an important and valid aim within inclusive policymaking. However, it can also end up reproducing existing power structures and priorities, depending upon the composition of the group, and how 'consensus' is interpreted and executed. Be sure to revisit the findings from your stakeholder mapping exercise and pay careful consideration to existing hierarchies and dynamics between stakeholders, to make sure that your shared understanding of consensus is truly inclusive.

Success might look like:

→ A cyber policy that has been developed or implemented inclusively, with meaningful participation from marginalised stakeholders;
→ A cyber policy which, in its content, concretely reflects the needs and priorities of all stakeholders, including women and marginalised groups;
→ A cyber policy which does not harm marginalised groups, or further entrench the inequalities they face—for example, through gender or inclusion audits.

Stage 4 Implementation

Having been involved in the development of the policy and in refining its accompanying action plans and outputs, civil society and marginalised groups will have more of an incentive to support its implementation. The key priority at this stage is clarity about implementation and the relevant roles and responsibilities within the implementation period.

Things to do at this stage

- For transparency and accountability, **develop an implementation plan**, with clear pathways and junctures for marginalised groups to input. This should include:
  - A detailed schedule, with information on what the scope for input is at each point;
  - Regular progress reviews, which provide an opportunity for stakeholders to input, scrutinise and raise concerns.
- To ensure inclusivity is maintained through the process, **clarify roles and responsibilities, modalities and safeguards** to ensure that marginalised groups maintain a role in implementation. This could include:
  - Research on the potential impacts of implementation;
  - Building transparency and accountability mechanisms collaboratively;
  - Ensuring stakeholders' active engagement and gathering ongoing feedback to inform agile decision-making at each stage of implementation (this might overlap with the Monitoring and Evaluation Stage).

Extra considerations

- Implementation should ensure that language around inclusion is mainstreamed across the policy lifecycle. This could mean ensuring that implementation teams—and particularly thought leaders—are diverse and inclusive, for example through quota systems and direct measures to support the participation of affected communities. This could also be supported by the allocation of specific resources to those with expertise in intersectional gender analysis, who are responsible for providing technical guidance to ensure equality in implementation.

Success might look like:

→ A detailed implementation plan, with clear roles and responsibilities, timelines and accountability and communication measures for transparent information sharing.

Stage 5 Monitoring & Evaluation

This stage should happen in parallel to all other stages, rather than simply at the end.

Here, marginalised stakeholders should be given a key role in ensuring inclusive policy implementation, and identifying any weaknesses or gaps in existing legislation that are required to support implementation of cybernorms.

Things to do at this stage

- **Develop an inclusivity measurement framework**, or series of inclusivity metrics, to assess whether the process and ongoing implementation of the cybernorm policy is inclusive.
- **Establish a multistakeholder working group**, including representatives from identified marginalised communities, to be responsible for coordinating and implementing review processes.
- **Schedule regular assessments, reviews and moments for reflection and analysis** throughout the policy process, involving all stakeholders.
- **Proactively respond to assessment findings and feed lessons back into the process** as appropriate. This might include details of substantive policy differences, as well as instances of unmet commitments, or experiences of discrimination or marginalisation within the policy development process. This is critical for ensuring transparency and accountability.
- **Publish these findings and lessons learned** to ensure accountability and insight-sharing across different communities, countries and regions.

Extra considerations

- Bear in mind that monitoring and evaluation could potentially identify a need to amend policy, which would mean starting the process again from Stage 1. This is normal; policies are not set in stone.

Success might look like:

→ A framework for accountability is agreed and includes tangible metrics to assess progress against;
→ Lessons from scheduled/regular reviews and moments for reflection/ analysis are fed back into the process.

This tool benefited from the approach set out in *The Intersectionality and Cybersecurity Toolkit* (The Centre for Feminist Foreign Policy, Marissa Conway and Nehmat Kaur, 2022)

Tool 1

How to facilitate inclusive stakeholder mapping

This tool provides detailed guidance to ensure a rigorously inclusive approach to stakeholder mapping. Generally speaking, an inclusive approach to cybernorm policymaking should seek to meaningfully include all stakeholders, including but not limited to:

1. Those with a mandate, role, or responsibility in the process
2. Those with skills or expertise needed to inform the policy and operationalise it;
3. Those who could be disproportionately affected by the policy or its implementation—i.e. marginalised groups.

This tool focuses especially on those stakeholders that could be disproportionately affected by providing a series of questions or prompts for policymakers to facilitate their engagement in cybernorm policymaking process. Its purpose is to help policymakers depart from focusing on pre-existing networks of institutions and organisations - which generally have the greatest access to capital, power and resources - to think broadly and reflexively about the range of individuals or groups disproportionately affected by cybernorm policymaking.

Step 1 Initial stakeholder mapping

This first step provides a series of guiding questions to assist policymakers in conducting an initial mapping of the individuals or groups who could be disproportionately affected by cybernorm policymaking. Step 1 is intended as a preliminary assessment based on policy-makers' existing knowledge and desk-based research; it should be followed by meaningful and ongoing consultation with the stakeholders identified, as set out in Step 3.

To be most effective, the guiding questions below should be answered in relation to a specific cybernorm policymaking process: for example, the development or implementation of a national cybersecurity strategy or an issue-specific cybersecurity policy like a government vulnerability disclosure policy, policies relating to the protection of critical infrastructure or the establishment of a national incident response centre.

Guiding questions:

- What are the policy issues which you are seeking to address through the cybernorm policy development and implementation process?

- Who is positively or negatively affected by the policy issues you are seeking to address?
- Which individuals and groups are specifically and disproportionately impacted by the policy issues at hand? Are they disproportionately impacted on the basis of their identity, status or beliefs?
- Who has historically benefited or suffered a detriment as a result of attempts to address these issues via policy development and implementation? Have they been disproportionately impacted on the basis of their identity, status or beliefs?
- Of the groups identified, are there any who are impacted in a distinct manner because of their possession of multiple or intersecting characteristics?
- What are the met and unmet needs of different groups which you are trying to address through the cybernorm policymaking process?
- How could the needs of the above groups be exacerbated or remedied as a result of the implementation of the cybernorm policymaking process in question?
- What organisations, community groups or other entities exist that are working on the cyber-specific policy issues identified above? What organisations, groups or entities exist that are working on these issues as they relate to gender, sexuality and other inequalities?

Step 2 Identification of barriers

The questions under Step 2 are aimed at helping policymakers consider the barriers or other sensitivities which may prevent particular stakeholders from meaningfully participating and engaging in a cybernorm policymaking process.

The identification of barriers should be prioritised early in the mapping process and should be subject to validation and input by stakeholders—as described in Step 3—to understand the barriers they may face and different forms of accommodation they may require. These questions should be answered in a manner which is specific to different groups, and generalisations should be avoided. In addition to identifying barriers, policymakers are encouraged to pursue the inclusion of less-networked and less formally organised groups as well as better-networked and more formally constituted ones; this will help to ensure groups without access to forms of social capital, power and resources are included.

The guiding questions below are relevant to any stakeholder engagement process. However, they may require further thought where you are engaging with marginalised groups, who are exposed to patterns of systemic discrimination. Additional guidance on how to ensure the participation of marginalised groups is also included in Stage 1 of the Toolkit.

Guiding questions:

- Are in-person consultations arranged with sufficient notice, and at appropriate times of the day?

- Are consultations undertaken and any relevant policy materials shared in appropriate languages?
- Are consultations shared in advance to provide stakeholders with sufficient time to analyse and respond?
- Are inputs accepted in a range of formats?
- Is communication clear and legible for stakeholders with a range of experiences and expertise?
- Is it financially feasible for stakeholders to contribute time to engage in the process?
- Is it safe for marginalised individuals or groups to participate, or will they experience violence or repression as a result of expressing their views? If not, what alternative processes can be pursued to facilitate their participation, such as anonymous contributions or encrypted channels?
- Are the means of engagement suitable for stakeholders with different cultural traditions?
- What hierarchies and dynamics may exist between stakeholders that you should be aware of?

Step 3 Review & Consultation

Following the initial identification of stakeholders and barriers under Steps 1 and 2, policymakers are encouraged to establish contact with identified stakeholders and to consult them on the results of their initial mapping. The third and final set of questions are a series of prompts for policymakers to ask identified stakeholders.

In this step, policymakers should actively and openly solicit input to identify any gaps in their mapping as well as additional stakeholders who should be engaged. Policymakers should also seek to better understand the barriers and sensitivities identified and any accommodations which may be required for stakeholders to meaningfully participate and engage in the policymaking process. This consultation should be meaningful, with inputs driving the expansion or adjustment of the mapping.

Guiding questions:

- Is the mapping of the policy issues at stake and their impact on different marginalised groups accurate and up-to-date? Are there any negative (or positive) impacts which haven't been identified, or any disadvantaged groups which were not accounted for?
- Is the mapping of the needs of different marginalised groups and how these may be exacerbated or remedied through the policymaking process accurate and complete? Are there any potential impacts which were not taken into account?
- Has the mapping considered the situation of those stakeholders impacted

in a distinct manner because of their possession of multiple or intersecting characteristics?

- Are the community groups, entities or organisations included in the mapping representative of a range of identities and perspectives? Are there any groups or perspectives which are not adequately represented? Who else should be engaged?
- Is the mapping of barriers and other sensitivities experienced by different marginalised groups accurate and complete? Is the mapping specific to particular groups and does it avoid generalisations?
- What adjustments do you require to ensure your meaningful participation and engagement in the policymaking process?

Tool 2

Gender and Inclusion 101

This tool provides an introduction to the key terms and concepts underpinning inclusive multistakeholder policymaking. As terminology relating to equality, marginalised communities, and identity can differ across contexts, please read it as broadly and inclusively as possible.

Gender

Gender refers to the socially and culturally constructed roles, behaviours, and values associated with masculinity and femininity in a given time and place. Gender norms are changeable over time; they inform individual identities, social relations, and the distribution of resources and power in society. Although gender is often understood as expressing expectations regarding appropriate behaviour for men and women, gender is non-binary and diverse. It refers to people of all gender identities and expressions. Gender equality therefore refers to equal rights, opportunities, and outcomes for men, women, girls, boys, and people of diverse gender identities and expressions. Equal treatment on the basis of gender is a human right enshrined in international law.

Gender identity

Gender identity is the deeply felt understanding of one's gender. For some people, referred to as cisgender, this corresponds with the sex they were assigned at birth. Trans is an umbrella term referring to people whose gender identities do not sit easily with, or are not the same as, the sex/gender they were assigned at birth. Trans identities are diverse and often socially, regionally, and culturally specific. Diverse trans identities may include, but are not limited to non-binary, gender-fluid, transgender agender, third gender and/or gender-queer identities. Transgender men are people who were assigned female at birth but live, identify as, and are, men. Transgender women are people who were assigned male at birth but live, identify as, and are, women.

Gender Expression

Gender expression is the way people express and live their gender through their actions and appearance. People whose gender expression does not correspond with societal expectations (usually deriving from binary expectations of heterosexual masculinity and femininity) can also experience stigma, discrimination and violence, as can people of diverse gender identities. It is therefore essential to consider people of diverse gender identities, expressions, and sexualities in all aspects of policymaking, from multistakeholder participation to substantive policy content.

Sexual Orientation

Sexual orientation refers to an individual's emotional, physical, and romantic attraction to other people. Though sexuality is often understood in terms of heterosexuality (attraction to people of the so-called "opposite" sex) and homosexuality (attraction to people of the so-called "same" sex), sexuality is also non-binary and diverse. Though sexuality is distinct from gender, heterosexuality is often a key gender expectation of men and women and can result in experiences of stigma, discrimination, and violence for people of diverse sexual orientations. It is therefore essential to consider sexuality and gender together in all aspects of the policymaking process, including but not limited to representation.

Essentialism

Essentialism is a way of thinking about gender (and identity more generally) that assumes that gender identity, expression, and, often, life goals, values, and trajectory follows directly from a binary, biological understanding of sex. Essentialism therefore also assumes that all men and all women have identical needs, capacities, and wants to each other. Essentialist gender attitudes also tend to ignore or deny the capacities, wants, needs, and even existence of people of diverse gender identities, expressions, and sexual orientations. Essentialism often appears in policy creation and analysis in the form of gender stereotypes and binary thinking. This might include the assumptions, for instance, that women are passive, emotional and want to be/are mothers, while men are aggressive, rational, and primarily engaged with formal economic activities.

Intersectionality

Intersectionality is a concept—and analytical lens—for capturing the ways in which multiple forms of social power, relating to class, race, coloniality, nationality, ability, ethnicity, caste, sexual orientation, age, geographic location, and gender expression work alongside gender to produce patterns of marginalisation and exclusion.

The term was developed by Kimberlé Crenshaw, an American legal professor, drawing upon a long tradition within Black feminism. An intersectional lens understands that marginalisation and oppression are not the additive sum of distinct forms of discrimination (e.g. gender + race + class). Instead, marginalisation and discrimination are understood as experienced simultaneously and specifically.

Following this legacy, "intersectionality" goes beyond ideas of inclusivity and diversity (or, indeed, demography) to analyse the societal power dynamics and hierarchies that produce these patterns and experiences of marginalisation and discrimination. Addressing the expression and continuation of various forms of power (e.g. patriarchy, class inequality, white supremacy, colonialism, ableism, heteronormativity, cisnormativity, etc) in social systems and institutions is an important precursor to social change. Like cybernorm development, intersectionality is an ongoing process rather than an end-goal in itself.

Marginalised groups

When we talk about marginalised groups, we are referring to groups who are disempowered. This marginalisation is often an effect of systemic and historic discrimination, which can result in the marginalisation of entire groups or communities. International law recognises an extensive and open list of more than thirty grounds of discrimination. While marginalisation is often a consequence of discrimination, not all those exposed to discrimination can necessarily be described as marginalised. Though inequalities exist in all places, the specific way they work, and who they affect, differs from place to place. It is therefore important to work with civil society actors to understand how marginalisation works in relation to a specific context, rather than assuming a priori. This is how some aspects of marginalisation, and the needs and perspectives of particular communities, are missed.

Feminism

Feminism is a broad commitment to promoting gender equality, and addressing gender inequality, amongst women, men, and people of diverse gender identities, expressions, and sexual orientations. Feminism takes gender and sexuality, through an intersectional lens, seriously as forms of power and social structures that inform social, economic, and political life. In policymaking, feminism involves commitments to equality, collaboration, open dialogue, and intersectional solidarity. Feminism understands the process of making, implementing, and evaluating policy to be as important a site for advocacy and change as the policy outcomes themselves.

Tool 3

Mapping cyber norm processes

The development of voluntary non-binding norms for state behaviour in international cybersecurity started over a decade ago. Convened as purely intergovernmental avenues, the multilateral cyber norms-making processes are getting increasingly open to the participation of various non-governmental actors in norm-setting, operationalisation, and implementation.

This development of cyber norms at various forums is an ongoing activity. New spaces can emerge with time, and when the mandates of existing processes, such as OEWG, are renewed. The diversification of the norm-making landscape and the emergence of non-state actors as norm entrepreneurs has created even more opportunities for civil society, women, and marginalised groups to get involved in these processes. This engagement is essential, in particular, for bringing gender considerations into the cyber norms-making efforts and the possibilities and modalities for engagement are evolving in existing fora.

This tool aims to map existing cyber norm policy processes and to help identify key forums and possible avenues for engagement and influence, especially for organisations representing women and marginalised communities. Where relevant, the information on ongoing processes is provided in the context of past developments that shaped the current norm-making activities.

The mapping is structured based on the level of activity—national and international—and the nature of the stakeholders leading the process. The focus lies primarily on the processes that understand cyber norms as voluntary, non-binding commitments as opposed to binding treaties and obligations. However, when binding frameworks are closely related to the issue of international cybersecurity, the mapping includes information about these instruments. It offers a snapshot of the most relevant cyber norm-making processes and should not be considered an exhaustive list.

1. International level

1.1. International multilateral avenues: United Nations

United Nations 1st Committee: non-binding norms, international cybersecurity

The UN cyber norms development processes comprise two tracks dealing with international cybersecurity and responsible state behaviour in cyberspace: the UN Group of Governmental Experts (UN GGE) and the the UN's Open-Ended Working Group on security of and in the use of information and communications technologies (OEWG), both groups' mandates fall under the UN's First Committee, dealing with international threats to peace and security. While the OEWG process started more than a decade after the start of the first UN GGE, the outcomes of their work are interrelated and, to a certain degree, reinforce each other.

UN Group of Governmental Experts (UN GGE)

The UN GGE process was convened in 2004. Between 2004 and 2021, the group held six negotiation rounds, with four concluding with consensus reports. The outcomes of each GGE were built on the previous work, providing important milestones in the development and implementation of cyber norms.

The first GGE consensus report in 2010 acknowledged the need for states to agree on the norms of responsible behaviour in cyberspace. Without proposing any norms, it recommended dialogue on this matter. The most important outcome of the GGE work was produced in 2015 when the group agreed on eleven non-binding norms. Without imposing binding legal obligations on states, these voluntary norms serve as a set of generally agreed-upon expectations for interstate behaviour in cyberspace. This entails both positive behaviours to be enacted and negative behaviours from which states should refrain. The norms include:

a. cooperation between the states in developing and applying measures to increase stability and security in the use of ICTs and a prevention of harmful ICT practices;
b. consideration of all relevant information in case of ICT incidents;
c. expectation to prevent the use of State's own territory for internationally wrongful acts using ICTs;
d. cooperation in addressing criminal and terrorist use of ICTs;
e. respect for human rights and privacy in ensuring the secure use of ICTs;
f. expectation not to conduct or knowingly support ICT activity that damages critical infrastructure;
g. commitment of the states to take appropriate measures to protect their critical infrastructure;
h. commitment to respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts;
i. ensuring integrity of the supply chain and prevention of proliferation of malicious ICT tools and techniques with harmful hidden functions;
j. encouraging information sharing about ICT vulnerabilities;
k. commitment not to harm the work of the authorised emergency response teams and not to authorise emergency response teams' engagement in malicious activity.

After the endorsement by the UN General Assembly (GA) resolution 70/237, which called on member states to guide their use of the ICTs by the GGE report, the eleven norms have become a baseline for other processes dealing with international cybersecurity, such as capacity and confidence building efforts by the regional organisations. The next round of GGE negotiations in 2016-2017, however, could not build upon this success and ended up in gridlock, with states not able to further agree on the applicability of international law in cyberspace.

Following this lack of consensus in the GGE, the UN GA adopted two competing resolutions. One created the next—sixth—iteration of the GGE, while another established a novel process: the OEWG. In contrast to the exclusive nature of the GGE, which initially was composed of 15 countries with a further increase to 25 members in 2016 (without the engagement of any other member states or stakeholders in its meetings), the OEWG was open to any interested member states. The two tracks deliberated in parallel in 2019-2021. In May 2021, the sixth GGE consensus report reaffirmed the eleven norms of GGE 2015 and focused on their better understanding and implementation.

Open-Ended Working Group (OEWG)

The OEWG 2019-2021 produced a consensus outcome in March 2021. The Final Report included recommendations in relation to rules, norms, and principles of responsible state behaviour in cyberspace, the applicability of international law, confidence-building measures, and other issues. The second part of the OEWG outcome—the Chair's summary—reflected the issues where no consensus was reached and aimed at informing future deliberations on cyber norms.

Binding treaty: United Nations 3rd Committee, crime and criminal justice

In addition to the UN First Committee cyber norms processes, a separate UN track—Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC)—is currently dealing with the issue of cybercrime. In contrast to the cyber norms, which aim at creating non-binding commitments, the AHC negotiations are supposed to result in a binding treaty. Following its establishment by resolution 74/247 of the UN General Assembly, the AHC started its work in 2021, intending to adopt the treaty by February 2024.

1.2. Other international government-led processes

While the United Nations remains the primary avenue for engagement with the core global cyber norm-making processes, various international initiatives emerged after the adoption of the GGE 2015 report. Some took the eleven norms as a foundation for their work, and others created their own voluntary commitments. These avenues include multilateral organisations, e.g. **Group of Seven (G7)**, political associations like the **Commonwealth of Nations**, and government-established processes that gained international magnitude, such as the **Paris Call**.

The eleven norms of the GGE 2015 reports are at the core of the commitments of several multilateral fora. The **Group of 20 (G20)** in Antalya Communique recognised the key role of the GGE in developing norms of responsible state behaviour in cyberspace and committed to the eleven norms from the GGE 2015 report. Similarly, the **G7**, in its Declaration on Responsible States Behaviour in Cyberspace 2017, supported the promotion of voluntary cyber norms,

referring to the eleven norms of the GGE 2015 and the G20 Communique which endorsed them. The Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group further highlights the G7's commitment to continue working with governmental and non-governmental stakeholders on non-binding cyber norms. This commitment was further operationalised in the G7 Dinard Declaration, which established the Cyber Norm Initiative (CNI) to share best practices for implementing recognised norms.

The **Commonwealth of Nations**, in its Commonwealth Cyber Declaration (2018) committed to promoting voluntary norms for responsible state behaviour and developing confidence-building measures consistent with the norms of the GGE 2015 report. The Cyber Declaration is being implemented through the Commonwealth Cyber Programme.

The **Freedom Online Coalition (FOC)** is a partnership of 36 governments, working together to advance Internet freedom. Over the past few years, the FOC has issued various joint statements and recommendations related to cybersecurity. For example, its Recommendations for Human Rights Based Approaches to Cybersecurity represent a commitment of FOC states to approach cybersecurity in a human rights-centric way.

The **Paris Call for Trust and Security in Cyberspace** was announced by the government of France in 2018. The Call pledges to maintain cyber peace and stability and comprises nine principles: protect individuals and infrastructure, protect the internet, defend electoral processes, defend intellectual property, nonproliferation, lifecycle security, cyber hygiene, no private hack-back, and international norms. Despite being launched by a government, the commitments aim at both governmental and non-governmental stakeholders; in contrast to the GGE norms, which focus on state actors. Some of the principles, such as infrastructure protection, overlap with the UN GGE norms and can be considered an operationalisation and implementation of GGE work. Others constitute new public-private commitments in cybersecurity. As of August 2022, the call was supported by 81 governments, 390 civil society organisations, and 706 private sector entities.

1.3. International non-governmental processes

While the first cyber norms processes, such as GGE, constituted an interstate dialogue and shaped voluntary commitments by and for the governments, in the last several years, norm-making efforts have been getting increasingly pluralised. When consensus between governments becomes difficult to achieve due to political tensions, the actions of non-governmental stakeholders can complement intergovernmental work and potentially provide an alternative route for a more stable and secure cyberspace. Cyber norm development and implementation efforts by non-state actors have expanded the notion of cyber norms from voluntary interstate commitments to practical pledges by various stakeholders.

Private industry-led processes

The involvement of the private sector in the discussion on cyber norms started in 2017 with a proposal for the "Digital Geneva Convention" put forward by Microsoft. The proposal called for states to commit to several norms, such as limiting engagement in cyber offensive operations and proliferation of cyber weapons. It faced criticism for focusing solely on state responsibilities while ignoring the existence of various avenues for developing the norms for

states' responsible behaviour. By extending the proposals to industry commitment, Microsoft established the **Cybersecurity Tech Accord** in 2018. The Accord proposes several principles for the private sector to protect users, strengthen cybersecurity, and exchange cybersecurity partnerships. As of August 2022, the commitment was signed by more than 150 companies.

Another private sector effort in the development of cyber norms—the **Charter of Trust**—was launched by Siemens at the Munich Security Conference 2018. The Charter contains ten principles aimed mainly at industry and, up to date, has 17 private companies committed to them.

Other processes

The **Global Commission on Stability in Cyberspace (GCSC)** was established in February 2017 and comprised 26 commissioners from various geographic regions and stakeholder groups. Building upon the work of the GGE, the final report of the GCSC proposed four principles (responsibility, restraint, requirement to act, and respect for human rights) and eight norms for both state and non-state actors.

Internet Society's **Mutually Agreed Norms for Routing Security (MANRS)** initiative offers a voluntary set of technical commitments (actions) to improve routing security. Launched in 2014 with four commitments for network operators, it expanded in 2018 with the programme for Internet Exchange Points and CDN & Cloud programmes in 2020.

2. Regional level

Regional intergovernmental organisations

Regional intergovernmental organisations are instrumental in implementing the UN GGE norms, sometimes through their own cyber norms development processes. The regional efforts of organisations such as the Organisation of American States (OAS), the Organisation for Security and Cooperation in Europe (OSCE), the African Union (AU), and others can potentially have more institutional legitimacy among their members, offer a better understanding of cultural and historical context and regional priorities, and facilitate cooperation and capacity development tailored for their region.

Organisation of American States (OAS)

The OAS was the first regional organisation to acknowledge the need for confidence building in cyberspace (see the 2009 declaration by the OAS Committee on hemispheric security). The OAS produced its first set of cybersecurity confidence-building measures (CSBMs), which aimed at encouraging information sharing between state actors in 2018. The following year, the OAS CSBM proposal (2019) focused on cyber diplomacy and capacity building. The latest measures released in 2020 included 31 "traditional" and "non-traditional measures" covering a wide range of issues related to cooperation in cybersecurity. Notably, one of the traditional measures provides for the involvement of non-governmental actors, in particular, civil society, in the dissemination and discussion of the confidence-building measures.

Association of Southeast Asian Nations (ASEAN)

ASEAN member states committed to developing a set of cybersecurity norms for the region in 2016. In 2018, ASEAN ministers agreed to subscribe to the norms of the GGE 2015 report 'in principle', with ASEAN leaders separately expressing commitment to put operationalisation of the GGE norms at the core of ASEAN's regional approach to stability in cyberspace. The operationalisation of the GGE 2015 is one of the primary pillars of the ASEAN Draft Cybersecurity Cooperation Strategy 2021-2025. The strategy expresses ASEAN's outlined concrete steps, including the importance of multistakeholder capacity building, with reference to the GGE and OEWG reports (2021).

African Union (AU)

The African Union has taken very limited action to engage with the GGE 2015 norms or foster regional approaches to cyber norms development. While the Digital Transformation Strategy for Africa 2020-2030 proposes to support UN-led cybersecurity processes, the AU's approach to cybersecurity focuses more on cybercrime. In 2014, the AU adopted the Convention on Cybersecurity and Data Protection, a legally binding instrument. However, as of August 2022, the Convention is yet to enter into force, as only 13 states have ratified it out of the 15 ratifications needed. Some researchers even question whether the GGE 2015 cyber norms were made to fit for states on the African continent, where supply chains do not originate and where some countries experience a lack of capacity for incident response.

Organisation for Security and Co-operation in Europe (OSCE)

The OSCE's focus on cyber norms development lies in capacity and confidence building. Since 2013, the OSCE has developed two sets of Confidence Building Measures (CBMs). The first set, developed in 2013, provided for establishing the points of contact and communications channels, and the second one (2016), aimed at more predictability, improved communications, and better preparedness. In 2016, the OSCE started a project to address the challenges of CBMs implementation in cooperation with the Global Forum on Cyber Expertise (GFCE) and other partners. Recently, the OSCE Birmingham Declaration 2022 urged states to refrain from malicious activity in cyberspace and the infringement of human rights and called for further implementation of the CBMs.

European Union (EU)

The EU has been actively engaged in the GGE and OEWG discussions and has expressed its continued support for and commitment to the eleven norms of the GGE 2015. The EU cybersecurity policy implements many aspects of the GGE norms through various instruments, including policies and strategies and various binding instruments, such as the EU Cyber Diplomacy Toolbox, the Network and Information Security Directive, the EU Cybersecurity Act, and many others.

Shanghai Cooperation Organisation (SCO)

The SCO has a very different view on cybersecurity as "information security"; at UN negotiations, its members' positions have promoted the idea that the states have the right to control information within their borders. In 2011, some SCO members (China, Russia, Tajikistan, and Uzbekistan) proposed an "International Code of Conduct for Information Security" to the UN General Assembly. The Code was criticised for its ambiguity, heavy reliance on the concepts of national security, and potential impact on the freedom of expression and other human rights. The updated version of the Code presented in 2015 focused on equal rights of the states and the importance of internet governance. Both 2011 and 2015 proposals suggest that the Internet should be governed multilaterally as opposed to the current multistakeholder model.