Call for Submissions: Cyber and Critical Technology International Engagement Strategy (CCTIES)

GLOBAL PARTNERS DIGITAL

Global Partners Digital response

June 2020

About Global Partners Digital

The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities. Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

We welcome the opportunity to input into Australia's Cyber and Critical Technology International Engagement Strategy.[1] Our submission responds to three of the sets of questions set out in the call for submissions: 1) What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology? 2) How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests? 3) What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

Contact

Sheetal Kumar
Senior Programme Lead, Global Partners Digital
sheetal@gp-digital.org
+44 (0)20 3 818 3258

[1] https://www.dfat.gov.au/news/news/call-submissions-cyber-and-critical-technology-international-engagement-strategy-ccties

1. What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

Australia's key international cyber and critical technology objectives should be to promote a free, open and secure Internet, and inclusive and multistakeholder governance of cyberspace, to maintain strong cybersecurity relationships with all partners, and to contribute to meaningful digital inclusion through the development of cyber capacity regionally and globally in order to ensure a peaceful and stable cyberspace for all.

Underlying this, should be the following values and principles:

- **Openness:** This means that active measures are taken to enable participation in cyber policy processes by all relevant stakeholders and other efforts are taken to address obstacles that may prevent or discourage this participation.
- **Inclusivity:** This means that different views and interests of the relevant stakeholders are heard and considered, and deliberations are informed and evidence-based.
- **Transparency:** This means that discussions and deliberations are documented, and the inclusion and exclusion of inputs into cyber policy development processes and decision-making power and methods are made publicly available.
- **Human-centric approach:** This means that individuals and the exercise of their human rights underpin and drive cyber policymaking.

Australia's current international cyber strategy dedicates two of its substantive six chapters to "human rights and democracy online" and "Internet governance and cooperation", where the commitment to inclusive and multistakeholder governance is outlined.

In addition, Australia should consider providing an overall framing and vision for the strategy which incorporates its understanding of the role of non-government stakeholders in pursuing its objectives, and the importance of human rights, including gender equality, as cross-cutting themes.

Below are included examples of how the current chapters of Australia's current international engagement strategy intersect with human rights.

- **Digital trade:** Digital trade liberalisation and facilitation through free trade agreements and participation in international policy forums such as the WTO, OECD, APEC and G20 impact human rights, in particular privacy and data protection. They may also impact the rights and safety of journalists and whistleblowers. Therefore, trade standards designed to increase the flow and use of data for commercial purposes must also include adequate safeguards to protect human rights.[2]
- **Cybersecurity**: Strong cybersecurity standards protect human rights, but measures taken in the name of preserving security can undermine human rights. Therefore,

[2] EFF, "Trade Agreements and Digital Rights", https://www.eff.org/issues/trade-agreements

human rights and cybersecurity should be seen as mutually reinforcing and cybersecurity policies should not undermine human rights in the name of protecting national security.

- **Cybercrime:** Human rights can be violated as a result of cybercrime, and as a result cybercrime policy and legislation can discourage and therefore reduce the prevalence of cyber-incidents that result in breaches of human rights. Frameworks developed to prevent and respond to cybercrime will have different impacts upon a range of human rights – specifically the right to privacy and freedom of expression. Appropriate legislation, effectively and fairly enforced, can help enhance people's human rights. However, measures taken to deal with cybercrime can also undermine human rights. For example, proposals to weaken encryption and thereby the security of digital technologies through the development of "lawful access solutions" or "backdoors" in the name of addressing cybercrime also have an impact on human rights.
- **Technology for development:** The development and use of technologies which enable socio-economic development can directly impact people's lives and their human rights and therefore should be secure and rights-respecting by design, as well as tailored to the specific context where they are deployed.
- **International security and peace:** The increased use and dependence on digital technologies means that the use of digital technologies by states has a direct impact on human rights. A lack of agreement on how international law applies to cyberspace, and non-adherence to norms of acceptable behaviour can result in increased tensions between states and in cyberattacks, including on critical infrastructure, which impacts human rights.

2. How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

In order for government, industry, civil society and academia to cooperate to achieve Australia's international cyber and critical technology interests, processes which are inclusive of all relevant stakeholders should be instituted from the outset of the strategy and support its implementation.

Australia should commit to establishing a multistakeholder advisory board (or equivalent mechanism) for the implementation of the strategy. In the current international engagement strategy, the government committed to the establishment of an "Industry Advisory Group" focused on supporting Australia's international cyber engagement, and in particular Australia's engagement in digital trade discussions and forums. This should be expanded to a wider range of actors, including the technical community and civil society, who also have a stake and role to play in the pursuit of Australia's international cyber and critical technology objectives.

A multistakeholder mechanism could also support the identification of key areas where the government can cooperate with stakeholders to implement all aspects of the strategy, including

technology for development, Internet governance and forums relevant to discussions on international peace and security.[3]

Alternatively, dedicated multistakeholder mechanisms could be established to support the implementation of each of the main chapters of the future policy. Either way, the institutionalisation of multistakeholder functions and processes within government can support advisory functions which are holistic, transparent, accountable, resilient and build trust in the long-term. Guidance on good practice in engaging stakeholders in cyber policy can also refer to other sectors including the climate change or the environmental sector, open governance, health, conflict prevention and peace building.

3. What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

GPD has identified that frameworks to address international cyber and technology policy issues in a way which is open, inclusive, transparent and human-centric require the following six criteria to be met:

- An unambiguous commitment to promoting a free, open and secure Internet as part of the state's foreign policy;
- An unambiguous commitment to the multistakeholder approach of Internet governance as part of the state's foreign policy;
- An unambiguous commitment to the principle that state behaviour in cyberspace is governed by international law;
- The identification of relevant international and regional forums and policymaking spaces where co-operation on cybersecurity takes place, and where that foreign policy can be advanced.

In terms of good practice frameworks for informing policy development and implementation, the UK, Fiji and Chile provide examples:

- The UK has established multistakeholder advisory groups (MAGs) to support its engagement in international governance forums in international cyber discussions relevant to international peace and security.
- Fiji is currently aligning its national cybercrime legislation to the requirements under the Budapest Convention. As part of this process, the Parliament of the Republic of Fiji has opened a call for written submissions[4] on a cybercrime bill.[5] Online consultations are a good modality to engage stakeholders, and may be particularly useful in cases

[3] In "Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers", GPD outlines modalities for engaging stakeholders in both the development and implementation of national cybersecurity strategies: https://www.gp-digital.org/publication/involving-stakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/
[4] https://www.facebook.com/fijiparliament/posts/2800002650105159
[5] www.parliament.gov.fj/wp-content/uploads/2020/05/Bill-No-11-Cybercrime-.pdf

where bringing people together physically poses practical challenges or costs are prohibitive.

- Chile adopted its National Cybersecurity Policy in 2017[6] after seeking stakeholder input through an online consultation.[7] As part of the policy implementation, Chile is currently aligning its cybercrime legislation to the requirements of the Budapest Convention. The Parliamentary Commission of Public Security, in charge of leading the process, has held public hearings to collect different stakeholders views and inform the bill.

In addition, there are a number of examples of multistakeholder forums and initiatives initiated by countries and regional forums which have established mechanisms for multistakeholder engagement in cyber policy discussions:

- Paris call for Trust and Security in Cyberspace and the Paris Peace Forum: France's project to support multistakeholder dialogue includes the "Paris Call for Trust and Security in Cyberspace", or "Paris Call" which was developed in consultation with non-governmental stakeholders and the Paris Peace Forum, a holistic platform for global governance issues which brings together stakeholders and provides a space to review and discuss the Paris Call within the context of peace and security issues more broadly through open dialogue.
- EU Cyber Direct: this programme brings together governments and non-governmental actors from across the EU and beyond to explore the main issues surrounding international law in cyberspace, norms of responsible state behaviour and confidence building measures.
- Organization of American States (OAS): The OAS/CICTE Cyber Security Program hosts an annual symposium for the Americas region. The symposium is attended by different stakeholder groups and has become a space for civil society to engage with the OAS and to share their perspectives to the discussions. For example, civil society groups have been leading cybersecurity and human rights sessions since 2017.[8]
- Global Commission on Stability of Cyberspace (GCSC) and Global Forum on Cyber Expertise (GFCE): the Netherlands established the GSCS as a multistakeholder expert group to develop and propose cybernorms for the global community (from 2017-2019) while the GFCE acts as global platform for capacity building, and includes a advisory board comprised by civil society representatives, and working groups where members (including government representatives and private sector) and partners regularly engage in cyber capacity building discussions.

[6] https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf
[7] https://www.ciberseguridad.gob.cl/consulta-ciudadana/
[8] https://www.tedic.org/tedic-en-la-agenda-de-ciberseguridad-de-la-oea/