16 JUNE 2020

Cyber Affairs
Department of Foreign Affairs and Trade
CyberAffairs@dfat.gov.au

Re: Australia's Cyber and Critical Technology International Engagement Strategy (CCTIES)

Introduction

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. As part of this mission we operate a global Digital Security Helpline for users at risk to mitigate specific technical threats. We work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those who are most vulnerable. We also host RightsCon, the world's leading conference on human rights in the digital age.

Access Now, through its Digital Security Helpline, is a member of the Forum for Incident Response (FiRST), the leading global incident response network.[1] We are founding members of CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the incident response capabilities of its members and share information on threats that affect NGOs, journalists, and other human rights defenders around the world. We support emerging regional and community-based help desk efforts to further close the gap between those in need and mechanisms of support.

Over the past years we have contributed extensively to Australia's public consultations (both in writing and in person); we submitted input to Australia's International Cyber Engagement Strategy and we have been actively providing commentary and suggestions to the ongoing review of Assistance and Access Act (TOLA). In November 2019 we also submitted extensive comments to the 2020 Cybersecurity Strategy Consultation held by Home Affairs. We work with a network of Australian digital rights and human rights organizations that understand the critical nature of protecting the digital rights of users. We coordinate frequently with academics, technologists, and the private sector to advance Australia's human rights compliance in the digital age.

General remarks

First of all, thank you for your continued engagement with stakeholders and allowing us all a part in the shaping of Australia's direction in this critical field. Australia has been an active player in the cyber policy space internationally, notably because of its appointment of an Ambassador for Cyber Affairs, its role as an active participant and supporter of the UN Open Ended Working Group (OEWG) (including supporting other governments' participation and focusing on greater gender

[1] https://www.accessnow.org/first-digital-security-helpline/

diversity in UN cyber policy discussions), and its role as an active member of the UN's Group of Governmental Expert (GGE) on Advancing responsible State behaviour in cyberspace.

We welcomed when in 2017, Australia launched a new International Cyber Engagement Strategy, intended to expand on "how Australia will attain global responsibility and influence in cyberspace."[2] The strategy includes goals in eight subject areas ranging from human rights and democracy to cybersecurity. We should note that in response, Access Now wrote to Tobias Feakin, Australia's Ambassador for Cyber Affairs, explaining that while the strategy makes mention of the rights to freedom of expression and association, it fails to show similar regard for privacy, not referring to it as a right and making reference only to "arbitrary interferences" to privacy instead of unlawful, disproportionate, and unnecessary infringements.[3]

In November 2019, we submitted comments to the Home Affairs Department consultation on *Australia's 2020 Cyber Security Strategy — A Call for Views*. At the time we noted that while many of the goals in the strategy are laudable and seek to establish Australia as a regional and global leader, the framing fails to recognize how the government's own current actions, including engagement in government hacking and threats to encryption under the Assistance and Access Act (TOLA), actually run counter to the commitments in the document. However, the most alarming change that we observed in the 2020 Cyber Security Strategy is the departure from the 2016 commitment to championing an "open and secure Internet."[4] The departure from this language, paired with the overall emphasis on government's role and authority over domestic networks and cybersecurity products and services is a shift to the detriment of Australian consumers. The language of the 2020 strategy shouldn't be based on the premise that the commitments regarding championing an open and secure internet made in the 2016 plan have been met and therefore do not need to be reiterated.

We would encourage the same consistency and continuity for Australia's domestic as well as international efforts in the cybersecurity policy space. In the November submission to Home Affairs we noted that "...there is a continued need to develop and grow the Cyber Engagement Strategy, which should be reviewed and held to a public consultation in the short-term." We are therefore very encouraged by this consultation and would like to congratulate DFAT on the consultative approach it has taken towards this as well as the OEWG and GGE processes. We hope that this consultative process continues and deepens. We also are hopeful that the refreshed DFAT strategy on Cyber and Critical Technology International Engagement builds on the framing emphasised in the Freedom Online Coalition's February 2020 statement:

> "Cybersecurity is not just about the security of assets and information. Cyberattacks have also imperilled individuals' safety, both because some cybersecurity laws have suppressed human rights and fundamental freedoms, and because malicious actors have undermined individuals' safety online.

[2]http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html.
[3]https://www.accessnow.org/cyber-engagement-strategy-australia-overlooks-threats-user-rights/.
[4]https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security

> Individual security,– whether offline or online, – should be a core purpose of cybersecurity; a secure Internet is central to the respect for human rights in the digital context. Cybersecurity measures should reinforce the availability, integrity, and confidentiality of information. These are essential to the security of the individual, especially in the digital context where physical security and digital information can be linked."[5]

Additionally, we believe that the Australian Government should, at a whole-of-government level, seek to further the following recommendation made in the same February statement by the Freedom Online Coalition:

> "States need to develop and implement cybersecurity-related laws, policies and practices in a manner consistent with international human rights law, and seek to minimise potential negative impacts on vulnerable groups and civil society, including human rights defenders and journalists. This includes building, where appropriate, supporting processes and frameworks for transparency, accountability, judicial or other forms of independent and effective oversight, and redress towards building trust. It may also include embedding the principles of legitimacy, legality, necessity or proportionality into policy and practice."[6]

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?

As indicated above, we believe that there needs to be consistency between the domestic and international objectives on cybersecurity. While some conversation between the government bodies certainly exists, we would encourage DFAT to engage with Home Affairs at this stage to ensure that there is consistency and continuity in objectives — and that those objectives are fully reflective of the work that Australia seeks to achieve internationally.

Governments have increasingly framed privacy and other human rights as antithetical to public safety and national security, stigmatizing valuable digital security tools. As a result, cybersecurity laws and policies often interfere with human rights or adversely undermine the security they seek to improve. With respect to the expertise and goals of Access Now, we recommend that cybersecurity policies are formulated to be: **user centric**, **systemic**, and anchored in an open **and pluralistic process**.

[5]https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf
[6]https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf

Cybersecurity and human rights are mutually reinforcing objectives. Efforts to establish norms of state behavior that promote freedom and security have sometimes failed to reach consensus and states do not always adhere to commitments. Countervailing forces have resisted an expectation of restraint, even against the most harmful actions. Those norm setting efforts have so far achieved limited success in creating a common understanding or effective accountability. Moving forward, more emphasis must be placed on protecting individual security as a true building block of cybersecurity with state action to honor those commitments. **The protection of human rights should be at the heart of cybersecurity policy development.** And significantly, efforts on cybersecurity must be aimed at ensuring the functioning of the open internet as a global network that can help realise our human rights across all nations.

In our 2018 report *Human Rights in the Digital Era: An International Perspective on Australia*, we concluded our analysis of the cybersecurity environment with these four key recommendations:[7]

1. Commit to building cybersecurity policies and practices around central tenets of human rights, including the right to privacy. This includes compliance with the government's own Cyber Engagement Strategy commitments on human rights and democracy;[8]
2. Evaluate government hacking law and practice with the goal of either ending the practice or, at minimum, codifying statutory safeguards to protect human rights;
3. Ensure representatives from civil society and the public are meaningfully included in cybersecurity policy-making, including the ability to participate in drafting key documents; and
4. Strengthen data breach notification in Australia to ensure full compliance by the public and private sectors.

We would further encourage Australia to evaluate existing gaps in cyber norms and the failure by states in respecting and upholding them — particularly with regards to how this impacts human rights. As it stands, this makes us all digitally insecure, placing users at risk and vulnerable communities in jeopardy. Building out a mechanism for monitoring and reporting on violations of cybersecurity norms and the impact on digital rights is a key priority for civil society, and it should be a key priority for the Australian government.

What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific?

Digital Identity Programmes

While there are large risks posed by any technology that is deployed in a legal framework which is not built to protect individuals and their rights, at Access Now we have been particularly

[7]https://www.accessnow.org/cms/assets/uploads/2018/07/Human-Rights-in-the-Digital-Era-an-international-perspective-on-Australia.pdf

[8]https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_6_human_rights_and_democracy_online.html

concerned about Digital ID Programmes in the Indo-Pacific region. In 2019 we launched the #WhyID campaign together with an open letter to world leaders detailing our concerns.[9]

As noted in the open letter, most digital identity programmes follow a centralised and ubiquitous model, without delivering incremental benefits to users. The central digital identity is linked to multiple other IDs and purposes for each user. This framework provides an ability to track and log everyday activities and transactions of a user. The ongoing global health crisis has further demonstrated the risks posed by digital identity systems that centralize such sensitive personal information.[10]

High profile cases have demonstrated that these programmes can create the risk of 360 degree profiling and surveillance of users by governments and private actors with access to the databases associated with such programmes.[11] Such an ecosystem can be hugely detrimental to the fundamental right to privacy of users. The problem is accentuated in countries with a lack of comprehensive privacy and surveillance frameworks, compromised institutional standards, and weak independent enforcement. In such countries, financial incentives become stronger for governments and private businesses to delay and dilute privacy and data protection standards, while enabling risky digital identity programmes.[12]

Current justifications for these programmes are often theoretical, and programmes are deployed without sufficient supportive evidence of the promised benefits. On the other hand, the harms that are suffered by individuals through badly designed and implemented digital identity programmes are real and in many cases, irreparable. Unfortunately, marginalised populations suffer the greatest harm. These digital identity programmes are all too often designed and implemented without a recognition of regional and local realities and without the consultation of key stakeholders including the most vulnerable.

Internet Shutdowns

While we remain concerned about the adoption of technologies without adequate human rights safeguards, we remain equally concerned about the continued increase of government ordered shutdowns.[13] Whether a shutdown is aimed at quelling protests, stopping cheating during exams, or influencing an election, authorities will often target specific services. In some contexts, a government will impose a shutdown of mobile data, and in others will block both mobile data and fixed-line connections. A shutdown can block social media and impact only those trying to connect via mobile, or throttle access to only specific services. This sort of disruption impacts the safety and security of individuals and communities, blocking access to critical information and support.

[9] https://www.accessnow.org/whyid/
[10] https://www.accessnow.org/government-responses-to-covid-19-reinforce-the-need-to-ask-whyid/
[11]https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf
[12] We provided comments to that specifically in the last round of the Universal Periodic Reviews (UPRs). You can see the excerpt and links to individual country submissions here: https://www.accessnow.org/internet-access-digital-id-data-protection-spyware-upr-review-highlights-threats-to-digital-rights/
[13] https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf

Like previous years, India took the lion's share of internet shutdowns in Asia, with its record of 121 incidents, followed by Pakistan with five shutdowns in 2019. Indonesia had more shutdowns in 2019 while Pakistan had fewer, but other than that, it has been business as usual, with authorities routinely shutting down the internet for religious holidays and protests. Myanmar, China, and Tajikistan also joined the list of countries that shut down the internet in 2019. In China, the highly complex system of censorship made it extremely hard to detect and verify any instances of internet shutdowns. In the lead-up to the 30th anniversary of the Tiananmen Square protest, state-owned internet service providers (ISPs) in many provinces — including Guangdong, Shanghai, and Chongqing — reported brief internet shutdowns "due to technical problems."[14] Yet there was little transparency to reveal the reasons behind such a massive scale of network disruption. In Tajikistan, where the internet is considered a luxury due to the high cost and low penetration rate, the authorities slowed down the already laggy internet in response to civil unrest, further deteriorating the already poor access to the internet in the country.[15]

From 2018 to 2019, the number of shutdowns lasting longer than seven days increased from 11 to 35. Chad, India, Ethiopia, Bangladesh, Myanmar, Indonesia, Democratic Republic of Congo, Eritrea, Iran, Iraq, Jordan, Kazakhstan, Mauritania, Sri Lanka, Sudan, Syria, Tajikistan, Turkey, and Zimbabwe all cut off access to the internet for more than seven days. Chad, Myanmar, and India had the longest documented shutdowns in 2019: Chad had a 472-day shutdown, Myanmar had a 248-day shutdown, and India had a 175-day shutdown. This is a clear indication of the grave situation people are facing in the blunt and extended denial of their right to access information and freely express themselves.

Shutdowns remain one of the greatest threats to human rights and the exercise of democratic freedoms in the Asia Pacific region.

How should Australia pursue our cyber and critical technology interests internationally?

Regional engagement

Australia should continue to pursue a regional leadership role as a part of its international approach (more on that below). In the Asia Pacifc region, Australia should seek to engage and support civil society and technical communities in terms of cybersecurity capacity, as well as supporting their engagement with government actors on cybersecurity policy. As noted in the section above on technological developments and risks posed by them, there is a need to engage with regional leadership in order to support the development of rights-centered solutions to

[14] NetEase (2019, May 13). 运营商"组团"断网，月底的流量加油包不想卖了？Retrieved February 21, 2020, from https://3g.163.com/dy/article/EGHRU2160527L76N.html

[15] Internet users comprised about 18.3% of the Tajikistan population in 2015, with the monthly subscription for fixed broadband at $58 USD, according to the Internet Society (ISOC). Internet Society (2017, June). Tajikistan Internet Exchange Point Environment Assessment. Retrieved February 21, 2020, from https://www.internetsociety.org/wpcontent/uploads/2017/08/ISOC-Tajikistan-IXP-assessment.pdf

existing, and future, issues. In particular, Australia should work with its regional partners on developing the gender dimensions of cybersecurity. There is a growing importance of mainstreaming gender perspectives and women's intersectional diversity as outlined in the OEWG report.[16]

Australia should continue to support diverse engagement and input into bilateral cyber dialogues and/or statements wherever possible. In particular, we believe that the Australian Government's international engagement strategy should explicitly seek to promote civil society and other stakeholder engagement in bilateral and plurilateral cybersecurity policy discussions (including "track 2.0 diplomacy" efforts in the cybersecurity space), as well as seek to regularly encourage other governments to involve digital security specialists and civil society in their cybersecurity policy development and engagement efforts. For example, Australia can work together with other states on encouraging wider stakeholder engagement with the ASEAN Regional Forum as it increasingly focuses on cybersecurity as a key part of its agenda, and wider multi stakeholder involvement with the cybersecurity discussions at the Pacific Islands Forum.

International engagement

Engaging on the international space should be a top priority for all countries seeking to reinforce and support human right standards in cybersecurity discussions. Access Now has been an active part of the UN OEWG, and we would encourage the Australian delegation to keep up its work in consulting with stakeholders (local and international) and supporting regional engagement where possible. In particular we welcome the human rights centric approach adopted at the OEWG.[17] Stakeholder engagement must remain an essential part of the process if the outcomes are to be universally accepted, supported and monitored.

For more concrete language, in September 2019, we submitted the following recommendations to delegations engaged in the OEWG process:

Regarding the functioning of the OEWG, we recommend:

- **Better integration of the OEWG process with regional discussions:**
    - As many stakeholders have requested, reports compiled after the regional consultations of the OEWG (currently underway) need to be made public in order to foster debate and integration across all stakeholders. States need to confirm and work with the UN secretariat to ensure this becomes standard practice for all regional consultations and the work plan of the OEWG.
    - Remote participation channels set up for future OEWG meetings, particularly for December and onwards, would enable better regional representation, especially from stakeholders who face challenges traveling to such meetings.
- **Security researchers must be empowered to inform the technical discussions taking place through the OEWG**:

[16]https://www.accessnow.org/as-states-discuss-global-cybersecurity-at-u-n-we-must-act-to-protect-users/

[17]https://www.accessnow.org/to-keep-us-safe-global-cybersecurity-norms-must-be-human-centered-and-protect-rights/

- More information security focused initiatives and organisations need to be allowed into the OEWG process. We are concerned that the incident response community and those who work on digital security research and information security strengthening are currently unable to adequately provide their expertise into OEWG deliberations. It is important for the international community and OEWG-engaged states to understand the work that technologists do regarding threat modeling and base OEWG deliberations on their expertise.

- **Facilitate greater participation by non-government stakeholders:**
  - From the denial of registration to non-ECOSOC accredited non-governmental organizations - resulting in only a handful of NGO participants attending the meeting - to the failure to livestream the statements by non-governmental organizations**,** we do not believe the OEWG has met its goal of "more democratic, inclusive and transparent" deliberations. Funding and travel support, dedicated space and time for statements and interaction with states, and two-way sharing of NGO and State/OEWG resources and documents should become standard practice.

Regarding the substantive discussions at OEWG, we recommend:

- **Adequately integrate regional processes on cybersecurity:**
  - We encourage proposals from some States to ensure that capacity building, confidence building, and mechanisms within regional organizations and elsewhere are systematically brought into the OEWG agenda.
  - Many regional and other initiatives have already undertaken steps to formally indicate their support to the 11 voluntary, non-binding norms that the 2015 UN Group of Governmental Experts (GGE) put in place. The OEWG should take this into its agenda formally to continue to engage regional groupings and fora in order to encourage them to consider adapting the earlier norms prepared by the GGE and understand how such regional efforts have been progressing.
- **Avoiding the use of the OEWG to develop norms related to combating cybercrime**:
  - We support the concerns raised by several States that cybercrime related coordination does not require sustained engagement by the OEWG. Other processes such as multilateral institution capacity building and coordination efforts, regional mechanisms, and international legal instruments on cybercrime are already being implemented and the OEWG does not need to duplicate those efforts.
- **Building bridges between the international development and cybersecurity initiatives at the international sphere**:
  - Ensuring universal, open, and secure access to the internet globally is key to the realisation of the Sustainable Development Goals (SDG), and the OEWG can help mainstream this thinking, particularly amongst the many States that are not part of the GGE process. It should be on the agenda of the OEWG to examine how improved adoption of the existing commitments and voluntary norms on cybersecurity from UN discussions would protect and facilitate the realisation of the SDGs, particularly as the internet and communication technologies have become so core to societal and economic functioning.

- **Recognising and documenting the cybersecurity focused recommendations from UN human rights bodies:**
    - The OEWG should facilitate the participation of the UN human rights system, including Special Procedures and thematic rapporteurships (from the UN and regional human rights bodies) and the OHCHR. This should be to connect and document the specific cybersecurity related findings and recommendations from these initiatives that have come in their human rights reporting and norm guidance.
    - OEWG discussions must also take on board the specific declarations and norms accepted by the UN Human Rights Council and the General Assembly in its Third Committee resolutions, including on internet freedom (A/HRC/RES/38/7) and the right to privacy in the digital age (A/RES/73/179), and strive to advocate that any further norm development or enforcement around cybersecurity in the context of international peace and security respects these fundamental human rights. That should include understanding existing evidence around targeted disruption of internet communications as well as the human rights value of secure communication systems.

Conclusion

Through its consultative and transparent approach, Australia has become a regional and international leader in cybersecurity policy discussions. It is essential that in further developing its approach, Australia remains a key regional partner for civil society and regional governments, and continues to model a human rights centric approach to cyber space.

We thank you for the opportunity to submit these comments to the Department, and we would welcome further discussion on specific cybersecurity priority areas such as advancement of human rights centric cybersecurity policy and norms internationally, the protection of robust encryption standards and best practices for public and private sector vulnerability disclosure. We remain at your disposal for any further questions or inquiries.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact:
Lucie Krahulcova | Australia Policy Analyst | lucie@accessnow.org
Raman Jit Singh Chima | Global Cybersecurity Lead | raman@accessnow.org