Contribution from the Association for Progressive Communications to the Internet Governance Forum's Best Practice Forum on Cybersecurity
15 September 2018

1. How do you define a culture of cybersecurity?

A culture that does not see human rights and security as needing to be balanced, or traded. For us a culture of cybersecurity is one that is human rights-based, and that places the security of users, their data and their online communications at the centre of its concerns. It is a culture that is defined by trust in the security of the network, its protocols, and the devices people use to connect to this network. It is a culture that reinforces, rather than threaten, human security. We also see it as a culture that respects due process and international law, particularly human rights law. Such approaches are systematic, meaning that they address technological, social, and legal aspects together. It is also a culture that is rooted in the power of the internet to connect people across borders and other boundaries. As such it should not differentiate between national security interests and the security of the global internet. Cybersecurity is broader than national security. Efforts to present it as first and foremost a national security concern should be countered.

For us it is also important that a culture of cybersecurity implies security for ALL users, from those that use it via entry-level mobile handsets to those that in large institutions with sophisticated firewalls. It should be as concerned with the security of the least empowered users as it is with that of the powerful.

We are concerned that the discourse of counter-terrorism tends to dominate conversations about cybersecurity. Cybercrime is a far more common concern for most users. This discourse that conflates cybersecurity with combatting terrorism reinforces a state-centric understanding and culture of cybersecurity, which in turn entrenches a culture that justifies measures that violates the rights of users (e.g. through mass surveillance of online communications).

Finally, for us a culture truly concerned with the security of the network and its users, should respect digital security expertise, and the people that provide digital security training and tools, particularly to journalists and human rights defenders. At present these people and the work and tools they use are often criminalised or targeted by authoritarian regimes. This is totally at odds with a culture of cybersecurity for all.

2. What are typical values and norms that are important to you or your constituents?

- **Human rights** norms and values are important to APC and our constituents. Cybersecurity practices, policies, strategies, must put human rights at the core. Not treat them as inherently at odds with each other. These include a broad range of human rights, including privacy, freedom of expression, freedom of association, participation in public life, and economic social and cultural rights.
- **Integrating rights and security:** Promoting a rights-based approach to cybersecurity has to be rooted in both security concerns and human rights concerns.
- **Inclusion:** The norm of transparent and inclusive decision-making is vital to us and we do not see any justification for the elitism and exclusion that often characterises decision-making and policy-making related to cybersecurity.
- **Collaborative and multistakeholder approaches:** We believe that governments, civil society and the technical community should work together closely to ensure

cybersecurity for all. Civil society and other rights advocates, business and the tech community should recognise that states are responsible for protecting the rights and security of their citizens (which does include responsibility for national security) and engage with states constructively and, when necessary, critically.

- **End-user oriented:** Discussions about cybersecurity should be "humanised" in the sense that it needs to be stressed that the ultimate victims of attacks are human beings, not machines or states.
- **Everyone has the right to secure communications:** That means that they have the right to use encryption, to remain anonymous, to use pseudonyms, and to be trained in digital security skills.
- **Security by design:** Privacy by design, no back-doors, and so on. We do not believe that governments (nor anyone else) have the right to arbitrarily build-in or exploit vulnerabilities in order to monitor or interfere with personal communications.

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

Progressive techie movement: Many of APC's members were involved in an initiative where progressive technologists came together and talked about their rights and responsibilities. They do not deal specifically with cybersecurity, but they are concerned with end-users having the power to develop and control technology. https://www.apc.org/en/news/progressive-techies-declare-their-rights-and-responsibilities Here is an extract from one of their documents: "We want a shift in the underlying logic of how technology is created and used. **Instead of being used as a tool to divide and conquer, we believe technology must be taken back by the people and used as a tool of liberation.** That communities on the ground should have access to the power to develop, control, and own technology."

Digital security and safety training: Currently many of APC's members are actively involved in building, promoting and providing training in digital security skills and tools. APC's Women's Rights Programme provides digital security training for women's rights and sexual rights activists and defenders.

GCSC: APC participates in the work of the Global Commission on the Stability of Cyberspace through one of the Commissioners, Anriette Esterhuysen. We value that this initiative is working on concrete norms and that it addressed both state and non-state actors.

We have been encouraged by the efforts of the Global Network Initiative, and specifically, more recently, of Microsoft to get industry to collaborate and commit to a culture of cybersecurity and defense. https://cybertechaccord.org/

Freedom Online Coalition: We have been part of the Freedom Online Coalition's development of recommendations, copied below, for linking human rights and cybersecurity.

1. Cybersecurity policies and decision-making processes should protect and respect human rights.
2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.
3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.

4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.

5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.

6. Responses to cyber incidents should not violate human rights.

7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.

8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.

9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.

10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.

11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.

12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders.

13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity. https://freeandsecure.online/

We advocate for these to be taken up by intergovernmental and national processes. We also advocate for comprehensive protections for encryption/anonymity and privacy by design/default as a means of achieving a secure and stable internet.

NETmundial principles: We identify also with the content of the NETmundial statement on cybersecurity. It is broad, but we believe its framing is still relevant:

> "1. Security and Stability
>
> a. It is necessary to strengthen international cooperation on topics such as jurisdiction and law enforcement assistance to promote cybersecurity and prevent cybercrime. Discussions about those frameworks should be held in a multistakeholder manner.
>
> b. Initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments,
>
> private sector, civil society, academia and technical community. There are stakeholders that still need to become more involved with cybersecurity, for example, network operators and software developers.
>
> c. There is room for new forums and initiatives. However, they should not duplicate, but add to current structures. All stakeholders should aim to leverage from and improve these already existing cybersecurity organizations. The experience accumulated by several of them demonstrates that, in order to be effective, an

> cybersecurity initiative depends on cooperation among different stakeholders, and it cannot be achieved via a single organization or structure.
>
> 2. Mass and arbitrary surveillance undermines trust in the Internet and trust in the Internet governance ecosystem. Collection and processing of personal data by state and non-state actors should be conducted in accordance with international human rights law. More dialogue is needed on this topic at the international level using forums like the Human Rights Council and IGF aiming to develop a common understanding on all the related aspects.
>
> 3. Capacity building and financing are key requirements to ensure that diverse stakeholders have an opportunity for more than nominal participation, but in fact gain the know-how and the resources for effective participation. Capacity building is important to support the emergence of true multistakeholder communities, especially in those regions where the participation of some stakeholder groups needs to be further strengthened." http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

Inclusive and collaborative approaches to policy development: One of APC's members, has shared an experience of positive engagement with a national government (Chile) on cybersecurity legislation based on the openness of government to civil society input. Civil society contributed to discussions of amendments to the cybercrime law in the Congress. Rather than criticising everything the government was doing, they worked with the government and provided alternatives, finding ways in which they could obtain better cybersecurity measures that respect human rights. Through this, they were able to build their own capacity and also help the government to build its capacity and understanding with regard to human rights concerns.

We have also found that the norm to work with a multistakeholder approach is very effective if different stakeholders can come together in a manner that creates trust and that gives everyone equal space to speak, and listen. We apply this, for example, in the African School on Internet Governance, where cybersecurity is part of the core annual curriculum.

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?

The norm of multistakeholder approaches is every unevenly adopted. For example, participation from both international and India-based civil society organisations in the most recent Global Conference on Cybersecurity, held in Delhi in 2017, was severely restricted.

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

We are aware of examples that are quite localised, where at a local or national level, industry, law enforcement and rights advocates have collaborated in developing policy and regulation. This might not qualify as implementation.

Most of our experience related to digital security and implementing measures to ensure the security of users in particularly vulnerable communities, e.g. women’s human rights defenders.

7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?'

Yes, for a number of reasons:

- The divide is partly because of malicious actors weakening security for certain people, groups, or countries, for example government hacking, exploitation of vulnerabilities, weak security measures employed when handling sensitive personal data, etc. Dissidents, journalists, women, people who face discrimination based on sexual orientation or gender identity (SOGIE) and others are often targeted by malicious actors and therefore suffer from lack of security online.
- Lack of data protection laws to require protection of personal data and notice of security breaches.
- Digital security skills is another reason, but important to put this in a way that does not put the onus on the end user. Governments are not investing in cybersecurity awareness and capacity building, companies are not implementing privacy by design, so it's not fair to blame the user for not having the skills necessary.

Relevant publication:

A *rights-based approach to cybersecurity: Recommendations and considerations from a 2017 Internet Governance Forum pre-event*, by Deborah Brown and Anriette Esterhuysen https://www.apc.org/en/pubs/rights-based-approach-cybersecurity-recommendations-and-considerations-2017-internet-governance

About APC: The Association for Progressive Communications, established in 1990, has 58 organisational members and 33 individual members in 52 countries who are dedicated to using the internet and other ICTs for social justice and sustainable development.

Contacts:

Deborah Brown, Association for Progressive Communications (deborah@apc.org)
Anriette Esterhuysen, Association for Progressive Communications (anriette@apc.org)