A RIGHTS-BASED APPROACH TO CYBERSECURITY: A PIPE DREAM OR A CRITICAL MEANS TO A SECURE AND STABLE INTERNET?

Recommendations and considerations from an Internet Governance Forum pre-event held on Sunday, 17 December 2017

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

A Rights-based approach to cybersecurity: a pipe dream or a critical means to a secure and stable internet?

Written by:
Deborah Brown
Anriette Esterhuysen

Copy editor:
Lori Nordstrom

Layout design:
Cathy Chen

Acknowledgements

APC acknowledges and thanks the co-organisers of the event "A Rights-Based Approach to Cyber-security: A Pipe Dream or Critical Means to a Secure and Stable Internet?" as well as all the panellists for their contributions. The co-organisers were the Centre for Communications Governance (CCG) at the National Law University, Delhi, the Centre for Internet and Society, Derechos Digitales, the Citizen Lab, Global Partners Digital (GPD), the Internet Society (ISOC), the UN Office of the High Commissioner for Human Rights (OHCHR) and Privacy International.

We also extend our thanks to Mallory Knodel, Maud Barret Bertelloni and Shawna Finnegan for their contributions to planning, organising and recording the event, and to Eleonora Mazzucchi of the Internet Governance Forum Secretariat for her invaluable cooperation.

The authors also want to recognise Flavia Fascendini, Lori Nordstrom and Cathy Chen from the APC communications team for the production of this report as well as the pre-event publication: "Briefing document: Cybersecurity policy and human rights" https://www.apc.org/en/pubs/rights-based-approach-cybersecurity-pipe-dream-or-critical-means-secure-and-stable-internet

ISBN 978-92-95113-04-6
APC-201807-APC-R-EN-DIGITAL-294

About this report

A rights-based approach to cybersecurity has gained currency in recent years at multistakeholder processes like the UN Internet Governance Forum. Progress has been made at human rights-oriented forums like the Freedom Online Coalition, which has developed recommendations for a free and secure internet.[1] Yet at the same time, threats to cybersecurity are on the rise, with significant human rights implications. Massive data breaches violate people's right to privacy; malware attacks are targeting human rights defenders and journalists, and also paralysing hospitals and public services; draconian cybersecurity laws are being proposed that could have chilling effects on freedom of expression, in particular political dissent; and the spaces where decisions on cybersecurity are being made are increasingly militarised, opaque, and unaccountable to the public.

To further explore this conundrum, the Association for Progressive Communications (APC), together with the Centre for Communications Governance (CCG) at the National Law University, Delhi, the Centre for Internet and Society, Derechos Digitales, the Citizen Lab, Global Partners Digital (GPD), the Internet Society (ISOC), the UN Office of the High Commissioner for Human Rights (OHCHR) and Privacy International, organised a Day 0 event at the 2017 UN Internet Governance Forum. The event, entitled "A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet?", aimed to deepen understanding of the human rights dimensions of cybersecurity policy by 1) identifying what is meant by a human rights-based approach to cybersecurity, 2) mapping out current initiatives in cybersecurity and stability, 3) exploring the human rights dimensions of cybersecurity threats and initiatives, and 4) identifying possible approaches towards consolidating a rights-based and inclusive approach to cybersecurity.

The format for the event was four panel discussions on the aforementioned topics, with interactive discussions following each panel. Speakers and participants came from academia, civil society, government, international organisations, the private sector and the technical community.

This report, prepared by APC, includes overall reflections and recommendations based on discussions in the event, followed by summaries and key points from each of the panel discussions.

1. https://freeandsecure.online

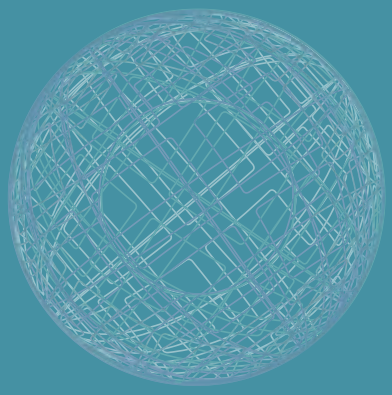


Table of Contents

Overall reflections and recommendations

At multistakeholder internet governance spaces, it has almost become a mantra to say that efforts to establish a secure and stable internet must respect and promote human rights. In reality, however, most cybersecurity policy development efforts tend to do little more than pay lip service to human rights. In fact, many contain provisions that threaten or undermine rights. It also seems that the general public alarm following the Snowden revelations has settled down. The internet has become a platform that no one really trusts completely, but that everyone uses anyway, as it is so intertwined with daily life. The wider impact of this mistrust is not yet clear and therein lies the danger, particularly with regard to the slow, global chilling effect it is likely to have on democratisation and online freedom of expression and association.

The Association for Progressive Communications (APC), together with the Centre for Communications Governance at the National Law University, Delhi, the Centre for Internet and Society, Derechos Digitales, the Citizen Lab, Global Partners Digital, the Internet Society, the UN Office of the High Commissioner for Human Rights and Privacy International, co-organised a Day 0 event at the 2017 UN Internet Governance Forum (IGF) to delve deeper and enable the articulation of a shared vision for a secure and stable internet that is rights-based, both at the level of policy, norms and standards and at the level of technical architecture and protocols.

In the course of the four panels that made up the event, "A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet?", presenters and participants came up with several recommendations towards consolidating such a shared vision, as well as some next steps for engaging in concrete, collaborative and solution-oriented actions. These recommendations and considerations were directed mostly, but not exclusively, at human rights advocates and civil society.

Definition and scope of the concept of cybersecurity

The internet should be seen as a global civic space. It crosses borders, connects people, institutions, countries. Cybersecurity cannot be equated with national security or achieved through a narrow national approach. At the same time, threats to national security posed by cybersecurity attacks or vulnerabilities should not be dismissed, nor should the responsibility of states for national security – provided they approach it as encompassing the security and human rights of their citizens – be disregarded. However, the fact that national security is implicated does not justify cybersecurity decisions being made under a shroud of secrecy. Some people proposed that the concept of human security could move us closer towards a rights-based approach. Others felt it might further the securitisation of discourse.

There was broad agreement that:

- Cybersecurity is broader than national security. Efforts to present it as first and foremost a national security concern should be countered.
- Civil society/human rights advocates should consider adopting a layered approach to cybersecurity with people at the centre, followed by, for example, the security of protocols, devices, data, networks and other critical infrastructure.
- 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.
- Promoting a rights-based approach to cybersecurity has to be rooted in both security concerns and human rights concerns.
- 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.
- Policy development and other efforts led by governments to address cybersecurity, even when connected with national security, should be open and inclusive.

Role players and processes

General concern was expressed about the lack of inclusion, particularly of civil society actors, in conversations about cybersecurity at global level, as well as in policy making at national level. Cybersecurity can only be usefully addressed with

the full involvement of all stakeholders. Trust in the network means security for everyone, not just for governments. One of the concerns for civil society about the potential of a treaty process on cybersecurity is that their participation in such a process is likely to be restricted and only possible through inclusion in national government delegations – a practice which very few governments currently embrace. Apart from the impracticality of the time it would take to negotiate a cybersecurity treaty, many raised the point about who would be setting the agenda for the treaty, and to what end. Most seemed to agree that a treaty would not result in greater respect for human rights in the context of security, but would instead lead to increased control by governments over their citizens.

Even when processes and institutions developing cybersecurity-related laws, policies and practices are closed off from public scrutiny, and civil society does not have a seat at the table, there are other ways to gain access and influence – for example, through informal meetings with representatives, through becoming involved in the work of standard-setting organisations, and through working with corporations where there is a shared interest. Suggestions included both general recommendations as well as specific advice:

- Cybersecurity processes need to be multistakeholder and inclusive, but also multidisciplinary. The need to connect rights advocates with technical and security experts was stressed repeatedly.
- States should not shy away from regulating the private sector when it is necessary to protect the public interest – for example, in connection with the import and export of technologies that can be used to violate human rights (as well as dual-use technology) such as surveillance technologies.
- Civil society efforts need to be infused with technical expertise. Civil society interventions in cybersecurity debates often suffer from a lack of accurate and up-to-date technical insight. Rights advocates can build their knowledge and capacity through working closely and consistently with technical experts.
- Civil society must participate actively in technology spaces where cybersecurity is the focus.
- Civil society and technologists often have shared objectives in keeping the internet secure and open, and can benefit from closer collaboration.
- Civil society should make an effort to engage at national level with technologists, business and law enforcement.
- Civil society organisations should collaborate with one another, find common ground and share the burden. They need to rely on each other to present common agendas, especially where access to processes is limited. Useful lessons can be learned from civil society's experiences engaging in trade and intellectual property negotiations.
- Be specific and prioritise. It is not useful to speak about human rights in broad terms. Demands should be precise, not just expressed as a broad demand for human rights. Issues should be prioritised to help focus the conversation across sectors and stakeholder groups.
- Avoid "us and them" or "good government" versus "bad government" rhetoric, as it undermines rather than builds common ground and collaboration.
- Use the IGF (and national and regional IGFs) as a space for discussing cybersecurity, taking stock of developments and trends, and promoting a rights-based approach.

Adopt a problem-solving approach

Too often discussions of cybersecurity focus on larger geopolitical issues and power relations rather than the issue at hand. One of the criticisms raised about there being so much focus on the development of a treaty is that it could move the discussion away from agreeing to concrete solutions to immediate problems. It was also pointed out that there is value in focusing on developing a normative framework in its own right, but also as a potential input into more formal international agreements or treaties at a later stage. Suggestions for solution-oriented steps included the following:

- Solve problems as they occur and do so in multidisciplinary and multistakeholder manners.
- Prioritise confidence-building measures. This is an area where governments can find common ground, and it can also help build trust that may lead to agreement later on regarding norms for responsible state behaviour in cyberspace.
- Demand greater investment in cyber defence. Governments are developing cyber offensive capabilities but they are not investing enough in defensive capabilities.

- Engage at national level. Norms at the global level are important, but national level policies are being developed and implemented in the absence of norms, so it is important (possibly more so) for civil society to engage at the national level.
- Civil society should move forward with a positive agenda and not just tell governments what they are doing wrong. Governments are looking for solutions and do not have all the answers, which presents opportunity for collaboration.
- Conduct research, to collect evidence and produce analysis on rights-related trends in cybersecurity policy and practice, including mapping the cybersecurity ecosystem.
- Establish norms for developers of technology to disclose vulnerabilities and patches used to address them.
- Build expertise, particularly in developing countries, across sectors and disciplines, and learn to speak one another's language in order to bridge silos.
- Capacity building is vital, for states and other stakeholders, so that they can engage effectively in cybersecurity processes.

Recognise and build on existing achievements and agreements

Working for a rights-based approach to cybersecurity does not start from a blank slate. Governments have made commitments to rights-based approaches to cybersecurity in multiple forums, nationally, regionally and globally. Governments also have human rights obligations under international law, which apply to their actions in relation to cybersecurity. Civil society and rights advocates should build on and leverage these commitments, including existing human rights mechanisms. There is certainly ground to build on to advance a human rights-based approach to cybersecurity. However, to translate commitments into practice, concerted efforts will need to be made to change the discourse around cybersecurity, to debunk myths, to connect people, movements and sectors, to break down silos, and to build capacity and trust among diverse actors who share this common goal.

Summary and key points from panels

Panel 1: What do we mean by a rights-based approach to cybersecurity? Is such an approach a pipe dream, or an essential means to a secure and trusted internet?

Panellists: Chinmayi Arun (CCG), Kathy Brown (ISOC), Marietje Schaake (European Parliament), Francisco Vera Hott (Privacy International)
Moderator: Peggy Hicks (OHCHR)

Defining a human-rights approach to cyber-security: Panellists characterised a human rights-based approach to cybersecurity as putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Such approaches need to address the technological, social and legal aspects together, and should not differentiate between national security interests and the security of the global internet. Human rights-based approaches to cybersecurity are very much linked to broader struggles for human rights – struggles which are continuously being undermined by new efforts to combat terrorism and other threats.

Exclusionary processes: A number of panellists pointed out that the context in which cybersecurity policy is developed contributes to the undermining of human rights and the security of the internet. Conversations often take place in closed spaces, without the participation of actors with human rights expertise or technical expertise. In some countries, especially in the global South, cybersecurity is viewed as a business development opportunity, with governments looking to improve security and companies looking to profit, but with no one raising human rights concerns.

Government remains the primary duty bearer, but business has a responsibility to respect rights: A human rights-based approach to cybersecurity requires government, as the primary duty bearer, to protect, respect and fulfil the human rights of all its citizens, which in this context means not

creating a false trade-off between rights and security. It also requires the private sector to uphold its responsibility to respect human rights, and can at times require governments to hold companies liable for not complying with their responsibilities. For example, governments should impose stricter controls over surveillance technologies and other technologies and systems that can be used for hacking, monitoring and tracking journalists and dissidents, by requiring a licence for the export of such systems and by ensuring that human rights assessment criteria are applied before licences are granted to these companies when they wish to export. Vulnerability disclosures were mentioned as another area in which government regulation should be welcome.

The gap between discourse and practice: Panellists pointed out a number of reasons why increased recognition of the importance of a human rights-based approach to cybersecurity has not been translated into practice.

- Advocates for a human rights-based approach are not specific enough. They tend to speak in broad strokes and principles, rather than referring to specific problems or policies.
- The cybersecurity/technical community and the human rights community speak different languages, which can obscure common agendas and solutions.
- Human rights advocates tend to come across as always pointing out problems, rather than working towards solutions.
- There is a lack of understanding by both civil society and government of the technology and technological systems involved in cybersecurity. In order to advance a human rights-based approach to cybersecurity, we need to understand both the law and the technology.

To treaty or not to treaty: Panellists also addressed the question of whether or not a new international treaty on cybersecurity is needed. There was agreement on the need to look at who is asking for a treaty and for what purpose. Some saw the debate on a treaty as a distraction from the need to focus on urgent problems that can be addressed immediately. By resorting to big treaty negotiations, we could just get farther away from solving actual problems, with the process caught up in whoever has the power at the time. Some people felt that the difficulties of the Group of Governmental Experts in achieving consensus (read more about this below) indicates how unlikely it is for treaty negotiations to produce results. Instead it was suggested that the focus should be solving problems where they occur, and bringing a multidisciplinary approach to solving them. Treaties may be useful, particularly from an aspirational perspective, but they take time to develop. Some felt that norms around good practices can be developed without the need for a treaty. It was also recommended that human rights advocates should reclaim the treaty discourse and refocus such debates on implementing the human rights treaties that are already in place.

Recommendations and considerations

- Look to solve problems where they occur, through multidisciplinary approaches and practical solutions such as human rights impact assessments at the technical level, rather than only speaking to human rights principles and norms.
- Different stakeholder groups and sectors should learn to speak one another's languages, not for the purpose of making compromises on principles, but to make human rights more understandable to one another and to work towards common objectives and solutions, where possible.
- Human rights advocates should identify positive agendas and solutions that they would like to see, so as to not only address problems with current policies or practices, but to contribute to agenda setting and prioritisation of issues.
- Capacity building is needed for stakeholders to better understand the technology, and specifically for actors in the global South to speak in their own informed voices.
- Governments should not be afraid to regulate companies when it is needed to ensure people's security and the security of the global internet.

Panel 2: Year in review: Overview of current initiatives in cybersecurity and stability

Panellists: Mehwish Ansari (ARTICLE 19), Madeline Carr (Cardiff University), Lea Kaspar (GPD), Kaja Ciglic (Microsoft), Markus Kummer (IGF Best Practice Forum on Cybersecurity), Chrystiane Roy (Government of Canada)
Moderator: Irene Poetranto (Citizen Lab)

Through initial interventions, the panellists gave overviews of key initiatives relating to cybersecurity and stability that were either launched or saw significant developments during 2017. These included the UN Group of Governmental Experts (GGE), the Global Conference on Cyberspace (GCCS), Microsoft's Geneva Digital Convention, the IGF Best Practice Forum (BPF) on Cybersecurity, the Global Commission on the Stability of Cyberspace, and the cybersecurity initiatives of the International Telecommunication Union (ITU). A number of themes emerged from the discussion and are outlined below.

Global intergovernmental conversations on norms in cyberspace seem to have stalled: The most striking example of this is the 2016-2017 UN GGE, which failed to reach consensus on norms governing responsible state behaviour in cyberspace, specifically on the application of existing international law. The group ultimately did not issue a report, and the UN General Assembly did not adopt a resolution on the issue, as it had in previous years, in part because some governments do not want parts of international law, including human rights law and humanitarian law, to apply. The lack of agreement on the applicability of international law meant that issues on which there was consensus, like capacity and confidence-building measures, also had to be dropped. The GCCS also had difficulty producing an outcome document. The Indian government, which hosted the Conference, had taken the time to draft a "Delhi Declaration"[2] for all participants involved, but it was dropped in favour of a less controversial chair's statement, which was rather weak on human rights. Compared to the outcome document from the previous GCCS in 2015, which included strong commitments to human rights and to the multistakeholder approach, this also marks a regression. The feasibility of an international treaty on cybersecurity must be viewed against this political backdrop, in which some states are negotiating to preserve their own interests, or the security of their own regimes, rather than the security of their citizens, not to mention internet users at large, and there is increasingly less common ground among actors.

Processes and institutions are increasingly securitised, opaque and exclusionary: Discussions on norms for ensuring security in cyberspace are increasingly government-led and dominated. As a result they are mostly securitised, and framed in terms of threat narratives. The spaces in which these discussions are taking place are generally closed, not transparent, not very inclusive, and difficult for civil society to engage in. The lack of inclusiveness and transparency in discussions on cybersecurity runs counter to the multistakeholder approach to internet governance and, critically, excludes the expertise and monitoring required to protect human rights. This was raised particularly in relation to the ITU, which is fundamentally an intergovernmental organisation where member states dominate the conversation and multistakeholder participation is minimal. The result is the alienation of the human rights expertise needed to ensure a rights-based approach to cybersecurity, with issues like privacy being co-opted to rubber stamp certain standards or policies that do nothing for the rights of users or, even worse, actually subvert these rights.

Reframing the debate in terms of human security: A strategy suggested for breaking through the impasse described above is to borrow the concept of human security from international relations, which includes human rights as a constituent element of national security. The state is still responsible for human security, but the human security approach asks different questions from those asked in a national security approach, such as:

- Security for whom? It needs to be brought down to the individual, since we are after all talking about the security of human beings.
- Security from what? Some actors see the goal of security as protecting themselves from political instability, from resistance, or from terrorism. Other actors see the goal of security as protection from human rights abuses.
- Security by what means? Through technology, through policy and regulation, through a treaty or through norms?
- What happens when the state itself, which in international relations is meant to provide security, becomes the source of insecurity?

New initiatives are emerging where traditional governance spaces are falling short: While UN and other ongoing international cybersecurity processes are stalled, other actors, like Microsoft

2. This draft declaration is not to be confused with the Delhi Communiqué that was eventually published by the Global Forum on Cyber Expertise: https://www.thegfce.com/documents/publications/2017/11/24/delhi-communique

and the Global Commission on the Stability of Cyberspace, are putting forward proposals and ideas for potential responsible rules of behaviour for nation states and non-state actors, focusing on the importance of accepting international law as applying in cyberspace. The Microsoft proposal additionally puts forward the idea of an international independent attribution unit and stronger commitments from private sector companies. The IGF BPF on Cybersecurity has also been trying to break down silos among stakeholders and foster a bottom-up convergence-seeking process on aspects of cybersecurity, like the contribution of cybersecurity to the Sustainable Development Goals.

Treaties may be useful, but it will take time to get there: Certainly the aspirational goal of having a treaty is to be appreciated, but we need to do something now, and cannot wait until we have a treaty. The Microsoft proposal of an attribution centre provides an interesting and concrete way of moving forward..

Cybersecurity frameworks and capabilities are being developed rapidly at national level: While discussions of global norms are critical for the future stability of cyberspace, the most pressing threats to human rights in the context of cybersecurity are happening through national laws and policies. Over the past year, Microsoft observed over 300 individual new pieces of legislation in over 100 countries, mostly based on national security principles. In addition, there is a dramatic expansion in cyber offensive capability across the world: over 40 countries have the capability to launch attacks. Therefore it is necessary to engage in national processes by working with governments, trying to shape those policies and legislation to integrate human rights concerns. However, global norms often guide national frameworks and provide a common language, so efforts to promote a rights-based approach at both national and global levels are equally important.

Recommendations and considerations

- The current geopolitical situation means that it is unlikely that intergovernmental processes will reach agreements on norms for responsible state behaviour in cyberspace. While this will probably not change in the short term, multistakeholder initiatives can continue to facilitate more inclusive and bottom-up discussions and advance thinking on norms and frameworks that reinforce a rights-based approach.
- More attention should be given to national -level developments, including through civil society and the technical community engaging with governmental actors who are rapidly developing frameworks and capabilities.
- Capacity- and confidence-building measures contribute critically to the stability of cyberspace and efforts should be made to ensure that progress in these areas continues, even when conversations on norms are stalled.
- Human security may be a useful framing, which does not deny the state's responsibility with respect to security matters in international relations, but applies an analysis that reinforces human rights instead of undermining them. Many people in the security field see focusing on human rights as a hindrance and aim to avoid it. Human security can help address this attitude, though confrontation between civil society, government and the private sector may be inevitable on this issue.

Panel 3: Deep dive on cybersecurity and human rights issues

Panellists: Maarten van Horenbeeck (Forum of Incident Response and Security Teams -FIRST)), Maria Paz Canales (Derechos Digitales), Luis Fernando García (Red en Defensa de los Derechos Digitales)
Moderator: Lucie Krahulcova (Access Now)

From a technical perspective, human rights and cybersecurity are deeply intertwined: both rely on technologies functioning in a trustworthy way. The challenge, however, lies in the point of view of the different stakeholders, and where investment is made as a result – for example, in defensive cybersecurity (making code more robust and secure), in building detecting controls, or in responding to threats. However, cybersecurity is not a matter of state versus state; it should be addressed at international level and ensure accountability for human rights which are universal and enshrined in international law. The securing of infrastructure, or looking after cybersecurity in both defensive and offensive terms, does not stop at the national level. Often, engineers simply build what their clients request, and are not aware of other issues, like the impact on human rights. Therefore, it is critical for civil society and the technical community to work

together to make technology more robust and respectful of human rights.

Privacy is not in conflict with security: The panel unpacked the debate of whether privacy is in conflict with security. From a civil society perspective, speakers asserted that privacy is in fact essential both for security and for an approach to cybersecurity that is centred on people. Just as people do not give up their right to privacy in the physical space to allow the government to keep them safe, they should not have to give up their right to privacy in the digital space. Speakers reflected on how states use fearmongering as a political tool. Under the guise of national security, they attempt to convince citizens to renounce their privacy. But when people do not have privacy from their governments, which in some places are known to be working with organised crime, it is not only their privacy that is in danger, but also their security. Cybersecurity needs to be moved out of the bubble of national security-justified secrecy and unaccountable behaviour.

Engagement with government on cybersecurity and human rights: Panellists reflected on their experiences in engaging with government around cybersecurity and human rights issues. A positive experience from Chile was shared, in which 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.

A less positive experience was shared from Mexico, which points to the limitations of including human rights language in policies when there is no mechanism to oversee or monitor compliance with these principles. Human rights language can legitimise a policy without putting in place any measures to ensure that the implementation of that policy is consistent with human rights norms and standards. In Mexico, the cybersecurity policy talks a lot about human rights as a result of civil society engaging in the process, in part in order to mitigate the criticism the government faced. Yet at the same time, the government spies on human rights defenders and journalists with malware attacks, which it justifies as necessary for the stability of the state.

Recommendations and considerations

More discussions and trainings within the engineering community on the human rights implications of technical choices are needed.

- At the same time, the human rights community can do more by participating in technical conferences and other places where engineers come together, to discuss the threats to human rights, not as principles but as concrete examples of the impact on end users. The Working Group on Human Rights Protocol Considerations at the Internet Engineering Task Force (IETF) is an example of a group that is working closely on identifying the human rights implications while building a new protocol.
- Assumptions regarding national security should be challenged. National security is currently characterised as a sacred sphere, where states can do whatever they want and the public cannot even discuss it or know what is going on. Given that citizens are so often asked to make sacrifices in the name of national security, it is crucial that the basis for those sacrifices are scrutinised for their necessity and proportionality; that there is independent oversight of responses to national security threats to ensure that they are justified; and that there is more transparency and as well as public debate to ensure that national security is not being equated with regime security.
- There is no one-size-fits-all approach to engaging with states on cybersecurity policies, but civil society can make better use of combined knowledge, understanding and diversity when engaging with all stakeholders to advance human rights.

Panel 4: Possible approaches towards consolidating a rights-based and inclusive approach to cybersecurity

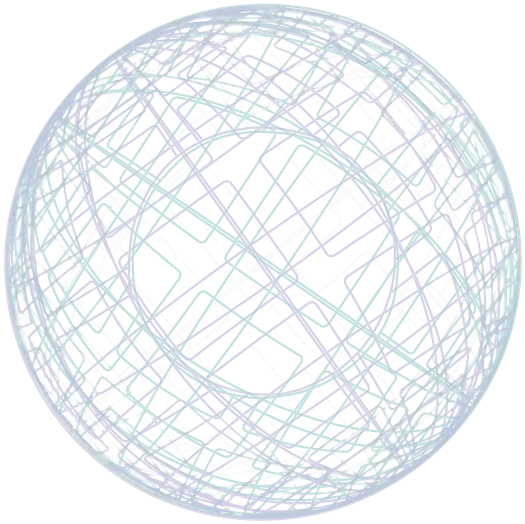
Speakers: Sunil Abraham (Centre for Internet and Society), Matthew Shears (GPD)
Moderator: Anriette Esterhuysen (APC)

The closing panel was a moderated discussion among speakers who have worked in the technical community, academia and multistakeholder spaces, reacting to challenges and suggestions that came up during the course of the event, based on their experiences, with the aim of charting out a consolidated roadmap for a rights-based and inclusive approach to cybersecurity.

Some key points regarding strategies that civil society can adopt that came up during the discussion include:

The need to infuse civil society ith technical expertise: It was suggested that civil society must "go multidisciplinary", getting engineers on its side, including by poaching them from corporations.

- Civil society activists must also be more engaged in technology spaces, and start thinking about themselves as hybrids, who understand the technology and the security concerns as well as the human rights concerns. This also requires that civil society "do its homework" and come prepared to debate technical matters and bring solutions to the table.
- The need to infiltrate cybersecurity spaces: Even when processes and institutions developing cybersecurity-related laws, policies and practices are closed off from public scrutiny, and civil society does not have a seat at the table, there are other ways to gain access – through informal meetings with representatives in hotel lobbies, for example. It is a marathon, not a sprint. Likewise, there are several standard-setting organisations where civil society is not present. This might mean that civil society has to work with corporations to gain access and influence.
- The need to find common ground and share the burden: There is an enormous amount of ground to cover, which can be made more surmountable if a set of civil society organisations that share a similar if not common theory of change can work together. This will also allow other NGOs willing to represent your agenda to collaborate and take on new battlegrounds which civil society has not traditionally participated in. To complement the idea that we need to work in synergy, trusting other organisations, we also need to build introspection in the way we work with each other and towards global goals.
- The need to avoid "us and them" rhetoric: Often in the international s phere, the so-called "good governments", which are promoting the internet freedom agenda, are the ones with the worst practices, happily violating rights online domestically without any redress. Using the "us versus them" dialogue often hinders attempts to create more of a common platform between global South and North governments, which results in a form of capture and co-opting.



APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS