PUTTING CYBERSECURITY ON THE RIGHTS TRACK

Acknowledgments

APC acknowledges the efforts of Alex Comninos, who was the lead researcher assisted by Mehar Gujral. Anriette Esterhuysen provided oversight and wrote and compiled the final report with input from Deborah Brown, Veronica Ferrari and Paula Martins. We also want to thank the APC members and partners who contributed their knowledge, perspectives and experiences to this study. Finally, we want to thank Mozilla for providing the financial support for the “Putting cybersecurity on the rights track” project, of which this research forms part.

TABLE OF CONTENTS

1. ABOUT THIS DOCUMENT

This document is a compilation of the outcomes of the research component of a small project entitled “Putting cybersecurity on the rights track” that the Association for Progressive Communications (APC) implemented during the course of 2019 with the participation of APC members.

2. THE PROJECT

"Putting cybersecurity on the rights track" was supported by the Mozilla Foundation. Its goal was to enable the APC network to develop a research and advocacy strategy to ensure that cyber-security policy and norms are influenced by civil society and progressive techie voices so that these policies integrate a rights-based approach.

The project built on the pre-event on a rights-based approach to cybersecurity organised by APC at the 2017 Internet Governance Forum in Geneva.[1] Based on the outcomes of that event, APC identified what it believed to be the primary challenges for civil society in relation to the cybersecurity landscape:

- The sidelining of civil society from cybersecurity processes.
- The fragmentation of cybersecurity processes.
- The rights and security "balance" myth.
- The "cybersecurity is a national security issue" myth.

1. Brown, D., & Esterhuysen, A. (2018). *A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet? Recommendations and considerations from a 2017 Internet Governance Forum pre-event*. APC. https://www.apc.org/en/node/34804

- A lack of common understanding and strategy among progressive non-state actors (rights defenders, civil society organisations, technologists, progressive internet companies and ethical hackers).

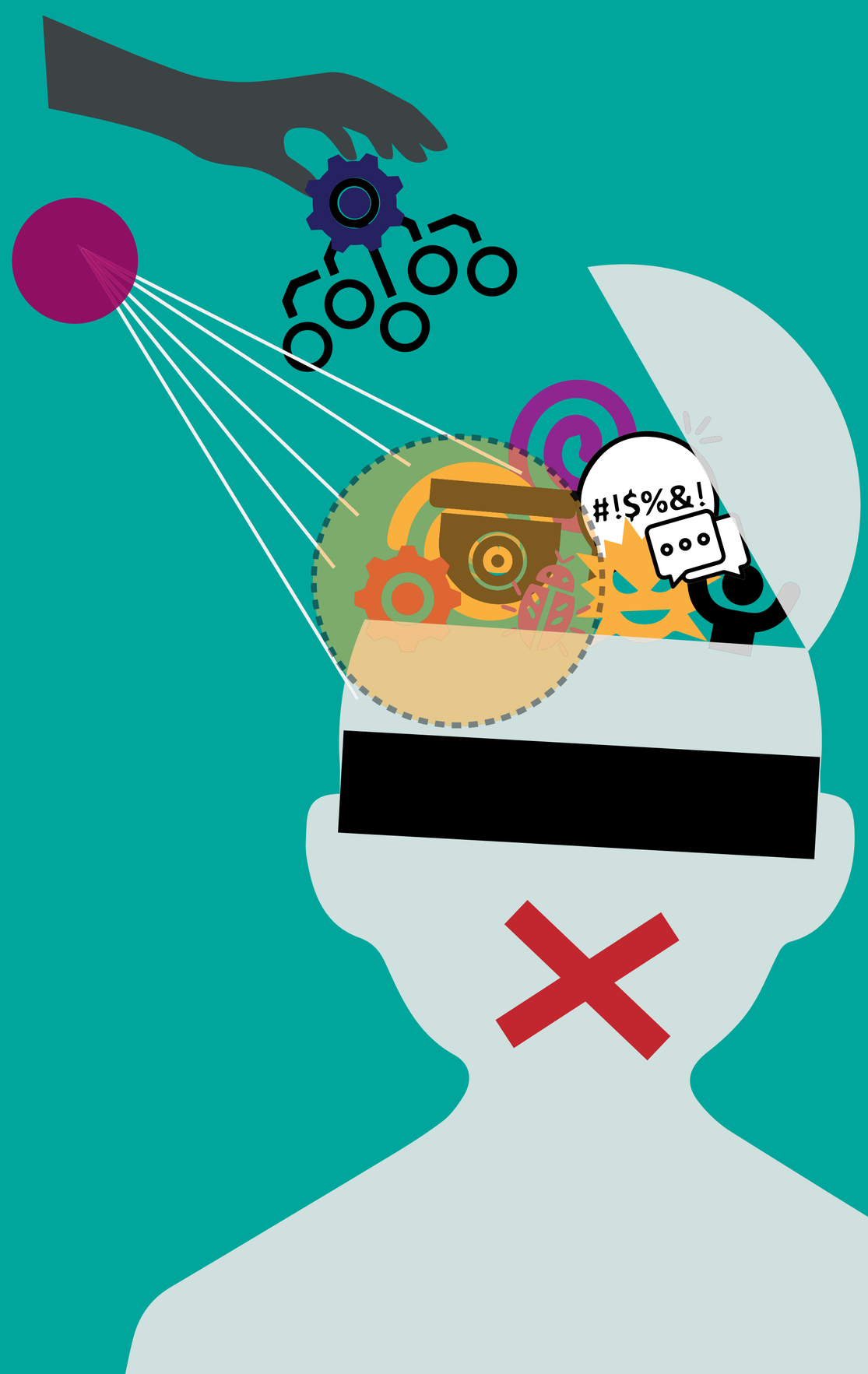
Strategies identified at this event by APC and its partners and members to address these challenges included:

- Deepening discourse: This can be done by connecting and combining the “rights” approach used by civil society organisations working in the digital space with the “network security” approach used by engineers and cybersecurity tech experts.
- Debunking myths: Through research and evidence, we can debunk the “security vs rights” approach, as well as the idea that cybersecurity should be dealt with primarily through “national security” strategies.
- Connecting people, movements, sectors: In particular, this involves bringing technologists and human rights experts together so that they see the challenges through one another’s eyes. We also want to use opportunities such as the Global Commission on the Stability of Cyberspace to develop rights-based norms.
- Moving out of civil society’s comfort zone: By promoting opportunities for civil society to participate in and speak at mainstream cybersecurity events, we will contribute to breaking down silos, gaining knowledge and developing tactics which will strengthen rights advocacy.

The “Putting cybersecurity on the rights track” project sought to move forward the implementation of some of these strategies through the development of the following key activities:

- Conducting a survey of APC members to establish a baseline of their cybersecurity-related perceptions, understanding and concerns.
- Mapping the ecosystem of who the key actors are and where critical cybersecurity decisions are being made (globally and regionally) to identify opportunities to advance human rights-based approaches to cybersecurity and identify where the main threats to human rights-based approaches to cybersecurity lie.
- Identifying and documenting case studies where APC members approached a cybersecurity challenge from a human rights perspectives in order to extract some lessons that can be shared.
- Visualising the ecosystem to map the issues, actors, institutions and processes making up the cybersecurity universe
- Building a longer-term research agenda.

“Electronic communications and media can be used to track, intimidate and manipulate people. Human rights is a political issue and as such, technology is just another tool in the political arsenal. People who advocate for the rights of the technologically excluded, might not be aware of these new weapons that can be pointed at them, to silence them or paint them in an unfaithful light.”



3. PROJECT ACTIVITIES

APC conducted a survey of members of its networks as part of the “Putting cybersecurity on the rights track” project. The respondents to the survey were APC members, partners and friends from countries including Australia, Cameroon, Chile, the Gambia, India, Kenya, Myanmar, Nigeria, the Republic of Korea (South Korea), South Africa, Spain, Uganda and Venezuela.

The respondents came from the following organisations: Asia Pacific Network Information Centre (APNIC), the Centre for Information Technology and Development (CITAD), Derechos Digitales, the Gambia YMCA Computer Training Centre and Digital Studio, the Global Forum on Cyber Expertise (GFCE), Internet Society India, the Kenya ICT Action Network (KICTANet), Korean Progressive Network Jinbonet, Myanmar ICT for Development Organization (MIDO), Nameshop, Net Freedom Pioneers, the Nigerian Federal Ministry of Communications, Pangea, Paradigm Initiative, PROTEGE QV, Right2Know Campaign, the Technical University of Catalonia, TICsLegal, Transworld

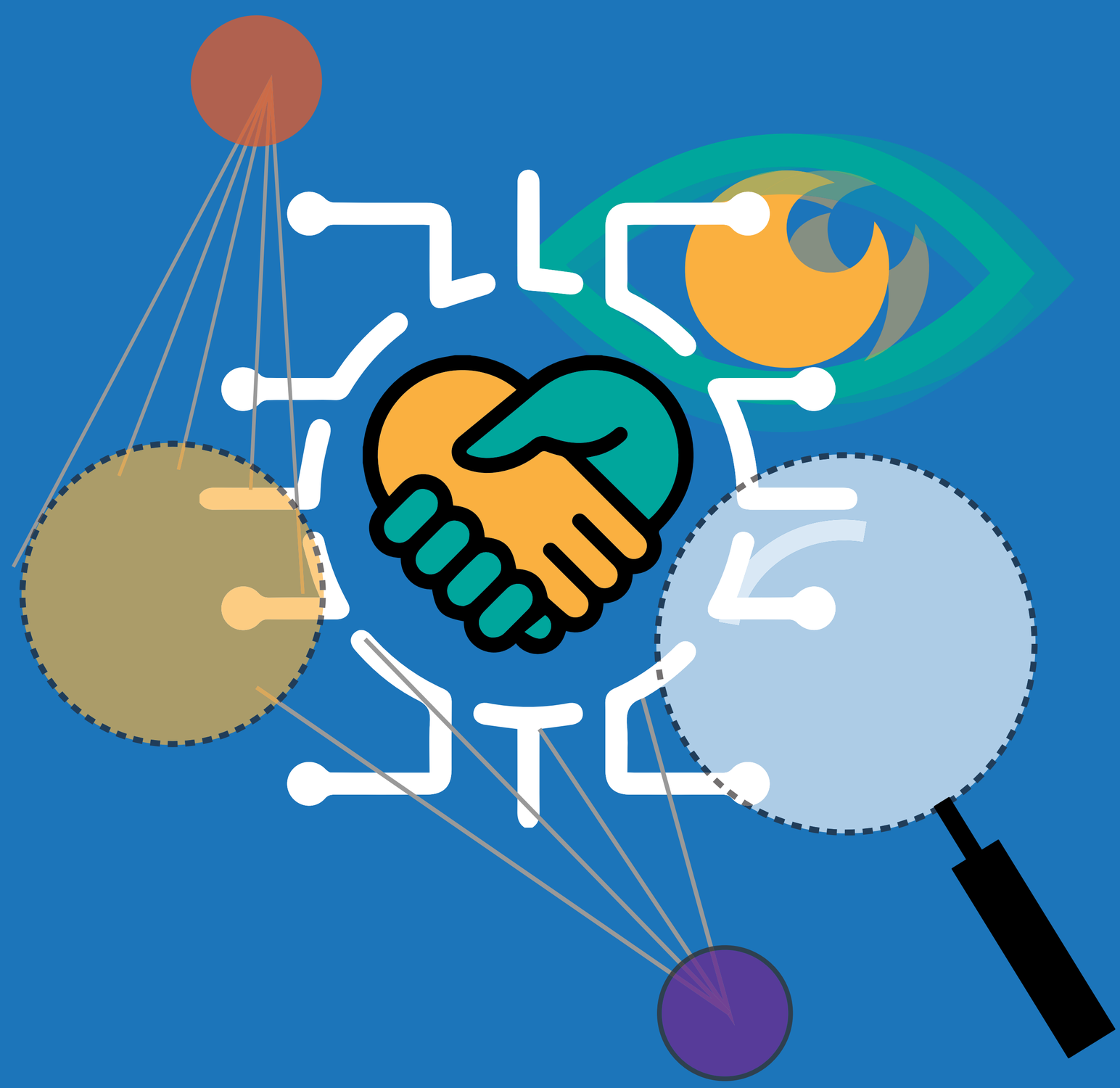
Africa Limited, Woman of Uganda Network (WOUGNET), Wikimedia South Africa, and Zenzeleni Networks.

Survey questions focused on their definition of cybersecurity, what threats they are experiencing, trends in the countries where they live, how they see the relationship between gender, human rights and cybersecurity, and what they would like to see in an APC cybersecurity and human rights research agenda. Appendix 1 includes a detailed report on the survey.

Section 4 below presents the key research findings, building on the survey results, complementary desk research and insights from further work in the area carried out by APC staff. It is also based on the outcomes of the December 2017 event mentioned in section 2 above.

As part of this project, three cases from within the APC member network of attempts to integrate human rights into cybersecurity initiatives or "putting cybersecurity on the rights track" were explored. Summaries of these case studies and lessons learned from them are presented in Section 5.

“Cybersecurity includes the necessary state of trust, both real and perceived, in the internet, networks, applications and devices that provides sufficient confidence in users for their continued use.”



4. RESEARCH FINDINGS

4.1 What is cybersecurity?

For civil society-based human rights defenders to be effective in their advocacy to “put cybersecurity on the rights track”, they need a deeper understanding of cybersecurity issues, processes and institutions. This includes knowing more about decision-making bodies, norm-setting institutions, standard-setting bodies, current cybersecurity initiatives and the technical aspects of security, threats and attacks. It also requires familiarity with the language of cybersecurity – terminology, jargon and tone. And ultimately, it will require a new language, with new terms and concepts that assert and make visible the links between cybersecurity and human rights.

Two concurrent trends have foregrounded cybersecurity: the increased dependency on the internet in people’s day-to-day lives, on the one hand, and, on the other, increased threats and attacks.

As these threats become more commonplace, sophisticated and severe, it is no wonder there is increased focus on strengthening cybersecurity by governments, industry and the technical community alike. However, these efforts to strengthen cybersecurity often "ignore the human rights dimension, or worse, view human rights as an impediment to cybersecurity."[2] This assumption is both dangerous and misguided. Civil society organisations, human rights defenders, journalists, and many others working for social justice are frequent victims of attacks and threats from both state and non-state actors. Cyber-insecurity limits the extent to which the internet is trusted as a vehicle for freedom of expression and association, for the exercise of civil and political and social and economic rights. To make matters worse, often the responses by states increase insecurity for civil society actors – such as, for example, restrictions on the use of encryption tools. Cybersecurity is clearly a human rights issue, and should be treated as such.[3]

There is no universal definition of cybersecurity, and the different approaches to defining or describing it reveal how politicised the concept is. It can mean the security of the digitised information and communications – including secrets – of states and companies. It can also mean being secure from crimes that are committed through the internet, or that target digital information and communications systems. It can also simply refer to the security of internet infrastructures, protocols and systems.

The term cybersecurity can be used to frame just about any threat and convert it into a cybersecurity issue. Depending on whether the term is being used by policy makers, activists, the media or civil society, there are a set of competing narratives and

2. Brown, D., & Esterhuysen, A. (2019, 28 November). Why cybersecurity is a human rights issue, and it is time to start treating it like one. *APC.* https://www.apc.org/en/node/35879
3. This section of the document draws extensively on the article by Deborah Brown and Anriette Esterhuysen cited above.

issues falling under the label of cybersecurity; they tend to involve a combination of information security issues and threats, threats to corporations and property, threats to "national security", as well as threats to human beings (including citizens and civil society).

From the perspective of "putting cybersecurity on the rights track", the definition developed by the "Internet Free and Secure" working group of the Freedom Online Coalition (FOC), which was composed of technologists, human rights experts and government representatives, is instructive. Drawing on the International Organization for Standardization 27001 standard,[4] they define cybersecurity as "the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline."[5]

From the survey of APC members (see Appendix 1 for a detailed report on the results), it is evident that APC members feel that gender needs far greater consideration in cybersecurity. The point was also made that cybersecurity looks different to different people or groups. Women confront different threats online, such as harassment, which is not usually considered in cybersecurity design. People who access the internet via mobile phone face different threats to those who use computers and need different solutions.

In response to a question on how they define cybersecurity, some APC members offered a purely technical definition of cybersecurity; for example, maintaining the "integrity and stability of data and networks", and "safeguarding internet systems from

4. https://www.iso.org/isoiec-27001-information-security.html
5. https://freedomonlinecoalition.com/working-groups/working-group-1

compromise". But most of the definitions they proposed had both a technological and human focus – for example, "Cyber-security is the protection of the internet [so] as to ensure that people are safe when they use it and that no harm comes to them because of the way other people are using it."

Privacy, safety and trust were other themes that recurred in the definitions people put forward. Some definitions also incorporated security both online and offline.

Responses touched on the notion of stability as being an expression of security. The Global Commission on the Stability of Cyberspace (GCSC), which very deliberately focuses on stability, not just security, defines cyberstability as follows:

> Stability of cyberspace means everyone can be reasonably confident in their ability to use cyberspace safely and securely, where the availability and integrity of services and information provided in and through cyberspace are generally assured, where change is managed in relative peace, and where tensions are resolved in a non-escalatory manner.[6]

One of the respondents described the complex and multi-layered nature of cybersecurity: "Security only exists in layers, and some of them are organisational and social, while most of them are purely technical."

The Feminist Principles of the Internet[7] do not have a principle dedicated to security, but make several references to the importance of being secure and safe online.

6. https://cyberstability.org/report/#note-13
7. https://feministinternet.org

The African Declaration on Internet Rights and Freedoms (APC and APC members contributed to the drafting) addresses security and stability, together with resilience, in its ninth principle:

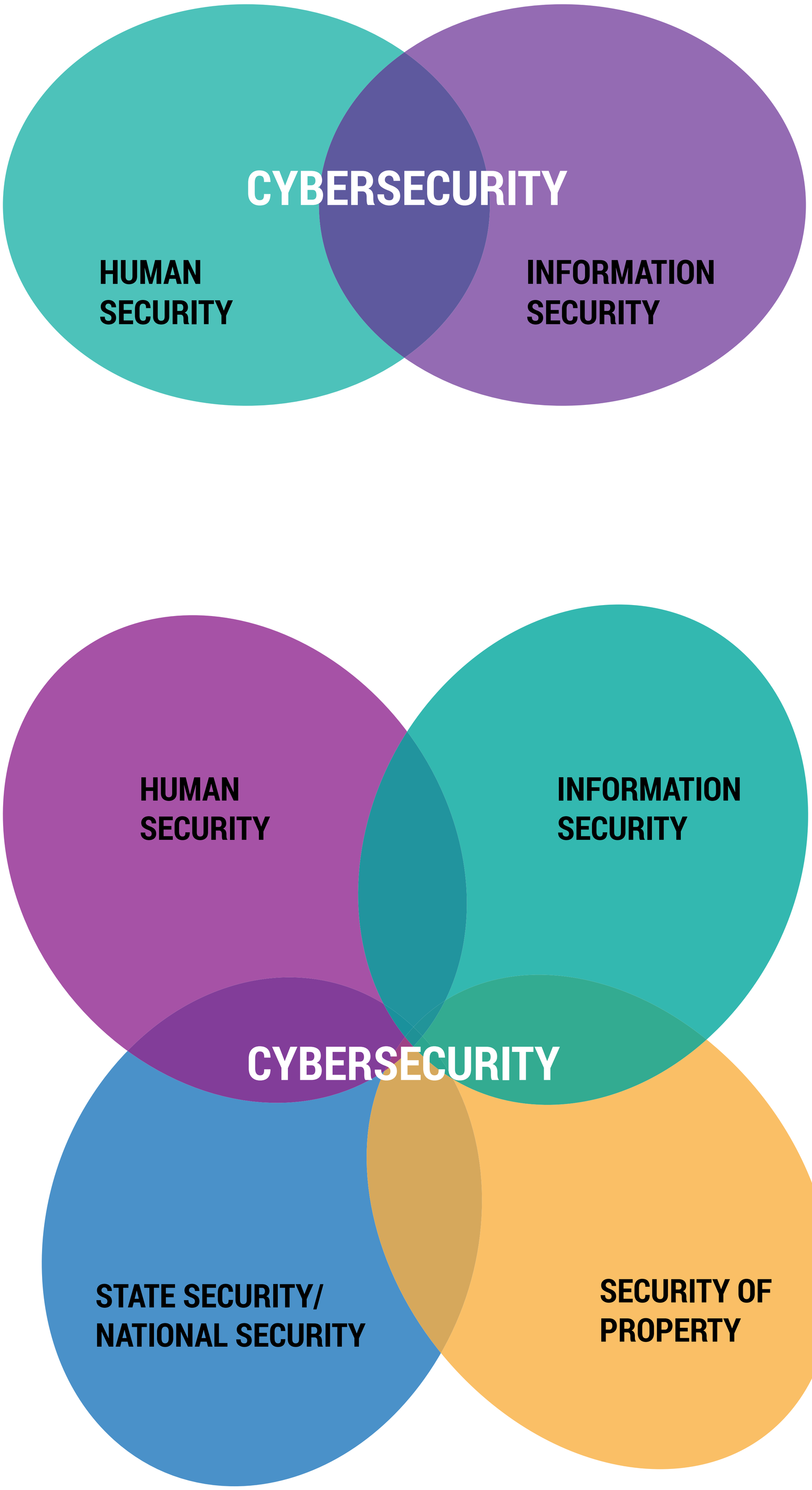
> Security, Stability and Resilience of the Internet: Everyone has the right to benefit from security, stability and resilience of the Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network.
>
> Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet. Unlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet.[8]

What is cybersecurity securing?

"Security" usually involves a reference to something that can be threatened or protected. When we talk about cybersecurity, are we talking about the security of the state, of private property, of the environment, of human beings, or of just information? We should be talking about people, not just information.

One way of looking at the scope of cybersecurity and deciding what works best for APC is to define it as the space or terrain where information security and human security overlap. Privacy International's definition of cybersecurity does this well: "Protecting and defending individuals, devices and networks should form the basis of any cyber security strategy."[9]

8. https://africaninternetrights.org/articles
9. https://privacyinternational.org/learn/cyber-security


CYBERSECURITY
HUMAN SECURITY
INFORMATION SECURITY
HUMAN SECURITY
INFORMATION SECURITY
CYBERSECURITY
STATE SECURITY/ NATIONAL SECURITY
SECURITY OF PROPERTY

"Information security" has been used much more narrowly to refer to the security of technology and information: computers and devices, networks, and data information systems. Cyber-security is more than just the technical area of information security, it is more than just the protection of information. Cybersecurity should have people at its centre, rather than bytes and bits.

At the 2017 Internet Governance Forum pre-event[10] entitled "A rights-based approach to cybersecurity", there was broad consensus that:

> 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.[11]

APC adopts a human rights-based approach to cybersecurity, which sees cybersecurity through a substantially broader lens than just a technical one. Neither does it see cybersecurity as just focusing on state or corporate security.

Seeing cybersecurity through a wide lens can be beneficial. A broader definition of cybersecurity that embraces the notion of

10. The event was organised by 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.
11. Brown, D., & Esterhuysen, A. (2018). Op. cit.

cyberstability would have the benefit of drawing attention to issues that normally would not be seen as security issues, and thus not attract sufficient attention, such as monitoring and interception of people's communications. It can also serve to put humans at the centre of security. But a broader definition can also have negative effects, such as "securitising" internet governance issues, and thus bringing them under the national security agendas of states. This is discussed further below.

Cybersecurity threats: APC members were asked to reflect on what they saw as important cybersecurity threats. They were asked to list threats to them personally, threats to their organisations and to people they work with directly, as well as threats to civil society in general. Many felt that the threats were the same for all three categories, or listed overlapping threats.

Personal threats: Personal threats included surveillance from private and state actors, hacking and phishing by both governments and criminals, malware, data breaches and leaks, identity theft, fraud and theft of data, inadequate data protection measures, profiling and data collection, fake news, harassment and coordinated attacks against vulnerable people, hate speech online, and online gender-based violence.

Threats to organisations and co-workers: When asked to list threats to their organisation and those they worked with, threats listed by respondents were almost entirely the same as the personal threats mentioned above. Threats in this category not mentioned previously (under "personal threats") included distrib-

12. A distributed denial of service (DDoS) attack is a deliberate and malicious attempt to disrupt access to the targeted website or mail server by dramatically increasing normal traffic to this server. Cloudflare describes this as being "like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination." For more information visit https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack

uted denial of service (DDoS) attacks[12] and spam.

Threats to civil society: Threats to civil society largely overlapped with personal and organisational threats but included the use of technology for manipulation through misinformation or targeted news feeds, or monetising harmful content through business models based on advertising revenue (sensational or violent content has often attracted millions of clicks by the time platforms choose to respond to requests for removing the content), as well as "securitisation" by governments of cybersecurity threats. As discussed above, this is used as a rationale for surveillance of people's communications and use of the internet, as well as content control.

National, regional and international threats: Respondents were asked to list national, regional and international threats. Again, the threats they listed overlapped almost completely with the threats mentioned above. A recurring theme with regard to national and regional threats was lack of data protection frameworks in many countries – and globally. National and regional threats not mentioned above included signal jamming and internet shutdowns.

International threats also largely overlapped with new threats mentioned, including state-sponsored hacking, software backdoors, "opaque proprietary systems that cannot be examined", and the military industrial complex.

The large degree of overlap among the threats mentioned suggests that a secure cyberspace is a global public good, and that threats from the personal through to the international are threats that affect all internet users.

CYBERSECURITY THREATS

PERSONAL THREATS

When survey respondents were asked to list threats to them personally, they mentionedsurveillance from private and state actors, hacking and phishing by both governments and criminals, malware, data breaches and leaks, identity theft, fraud and theft of data, inadequate data protection measures, profiling and data collection, fake news, harassment and coordinated attacks against vulnerable people, hate speech online, and gender-based online violence.

THREATS TO CIVIL SOCIETY

Threats to civil society largely overlapped with personal and organisational threats but included the use of technology for manipulation through misinformation or targeted news feeds, or monetising harmful content, as well as securitisation by governments of cybersecurity threats. As discussed above, this is used as a rationale for surveillance of people's communications and use of the internet, as well as content control.

THREATS TO ORGANISATIONS AND CO-WORKERS

When asked to list threats to their organisation and those they worked with, threats listed by respondents were almost entirely the same as the personal threats mentioned above. Threats in this category not mentioned previously (under "personal threats") included denial of service attacks and spam.

NATIONAL, REGIONAL AND INTERNATIONAL THREATS

Respondents were asked to list national, regional and international threats. Again, the threats they listed overlapped almost completely with the threats mentioned above. A recurring theme with regard to national and regional threats was lack of data protection frameworks in many countries – and globally. National and regional threats not mentioned above included signal jamming and shutdowns.

Cybersecurity decision making at national and regional level

The survey asked respondents to list the institutions involved in cybersecurity processes in their countries and regions and whether there were legislative instruments in place or under development. They were also asked to reflect on the nature of decision-making processes – in particular, whether they are inclusive of all stakeholder groups. Common factors that stood out for most respondents were that:

- Cybersecurity is generally the concern of multiple institutions in government and in most places there is a lack of clear coordination. This makes it very difficult for civil society to participate in and influence relevant processes, even if they manage to gain access in one way or another.
- Legislation is being developed in all countries covered by the research. In some places, laws are in place, but in most, they are being developed. There are often overlapping legal instruments.
- Cybersecurity decision making and policy at national level have negative, or chilling, impacts on human rights online in most places. At times, these impacts are direct and intended by repressive legal instruments. But in most cases, they seem to be indirect or unintended, resulting more from not enough consideration being given to human rights, than from states deliberately using cybersecurity to restrict rights. This is an important finding and suggests that there is a window of opportunity for civil society and other stakeholder groups to raise awareness, and to insert human rights considerations into cybersecurity processes.
- In response to the question on whether cybersecurity processes involve all stakeholder groups, most respondents said they did

not. It is clear that the multistakeholder approach that has taken root to quite a large extent in broader internet governance processes is not being applied consistently in the field of cyber-security.

4.2 Securitisation of cyberspace

Cyberspace, and as a result cybersecurity, are such broad concepts that people end up including all kinds of issues under the cybersecurity rubric. Issues that are very different in nature, such as credit card fraud, sexual harassment, recruiting of so-called terrorists, distribution of child sex abuse material, or ransomware attacks, are bundled together and seen as cybersecurity concerns, resulting in the "securitisation" of everyday internet challenges and internet governance concerns.

This securitisation can have a positive or negative effect. On the positive side, it can help attract the attention of policy makers to issues that are overlooked, such as harassment and other forms of online gender-based and violence. This heightened attention can lead to improved collaboration among business, the technical community and government in practical ways that increases the safety and security of affected people. But it can also lead to top-down state-centric responses that do not consider the participation of the people affected, or the social and technical aspects of the problem. It can result in securitised solutions which are not only not effective, but can create new problems and violate basic rights such as freedom of expression and association.
In the case of gender-based violence, these so-called solutions often infantalise women, positioning them as defenceless victims who are like children, unable to defend or protect themselves against violence, and who therefore need to be protected by the state.

Securitisation of an issue can result in it being viewed through a national security lens, thus changing the way the issue is handled and by whom. This can reduce independent oversight and public scrutiny of how the issue is handled as it is "in the national interest". This is the most dangerous consequence of securitising cyberthreats. It can lead to justifying disproportionate restrictions of rights, particularly the right to privacy. It can easily lead to those with power justifying authoritarian responses to securing the internet. The national security narrative encourages tolerance of these restrictions by users/citizens for the sake of the "greater good".

It is all too common for laws, policies and norms on cybersecurity to be developed with little transparency and participation. This means that these processes often lack monitoring and input from those with expertise in human rights. APC has called attention before to the fact that:

> Often, cybersecurity discussions happen in the confines of intelligence services, or other government or military agencies that are not subject to public scrutiny or oversight. […] As a result, cybersecurity law, practices and policies are often divorced from a human rights framework, and susceptible to abuse of power.[13]

13. Brown, D., & Esterhuysen, A. (2019, 28 November). Op. cit.

Cybercrime and cybersecurity: Separate but linked

One of the most common consequences of the securitisation of cyberattacks and threats is the bundling together of cyber-security and cybercrime. This is a narrative not only led by states; many in civil society also do not consistently recognise the difference. Most APC members who responded to the survey mentioned that legal instruments to address cybercrime and cybersecurity are being developed in their countries and in most cases these instruments do not distinguish between cybercrime and cybersecurity.

Efforts to put cybersecurity on the rights track should give very serious consideration to the differences between cybercrime and cybersecurity. Both are important and both have human rights implications. Perhaps the difference is that while cybersecurity is broadly and essentially a human rights issue, cybercrime is not a human rights issue, but efforts to address it should comply with human rights standards.

4.3 Developing a rights-based definition of cybersecurity and stability

Survey responses to the question on the relationship between human rights and cybersecurity conveyed a very clear message: cybersecurity is needed to protect human rights online. It is not only a human rights issue, it is a precondition to enabling people to enjoy and exercise human rights online. One respondent put it very succinctly: “Deprivation of my cybersecurity denies me the ability to defend human rights.”

Respondents pointed out that both cybersecurity and the broader exercise of human rights online are particularly dependent on respect for the right to privacy. Encryption is vital to both. A cyberspace where individuals do not feel safe and secure in transacting, expressing themselves, or working with others is an insecure cyberspace.

The survey results indicate that APC should build a rights-based definition of cybersecurity that is human-centric, embraces the notion of stability, and recognises that different people experience security and insecurity in profoundly different ways.

A possible approach would be to build on the contributions from APC members in response to the survey to revisit the GCSC definition of cyberstability and the FOC definition of cybersecurity, for example, inserting a gender angle into both. The Feminist Principles of the Internet could also consider developing a specific principle, or at least a strategy that addresses cybersecurity and stability from a gendered feminist perspective.

misogynistic safe educational
compromise online technology
knowing CIA prevention protecting continued
confidentiality platforms consequences issues
control beneficial safeguard various way trust
real navigate networks encounter perspective
ensuring tools safely events maintain offline
measures proportion electronic nature extent bad
transactions reuse technical digital respond economy
safety CYBERSECURITY threats
perceived both
means relates afraid remains stability global users
privacy everything else space all ensure protection
world theft under data reliable processed collection things
comes harm society concept internet defined
password use other state including infrastructure
applications communications sufficient
some integrity related fraud different aware
devices yourself cyberspace awareness availability
fundamentally people information

5. LESSONS LEARNED FROM APC MEMBER EXPERIENCES OF PUTTING CYBERSECURITY ON THE RIGHTS TRACK

APC conducted three case studies from within its member network of attempts to integrate human rights into cybersecurity initiatives or “putting cybersecurity on the rights track”. The case studies were from Bangladesh, Kenya and South Korea. All three case studies focused on integrating human rights concerns into cybersecurity efforts, but differed at the level of geographical and institutional context. The Bangladesh case study focused

on Bytesforall Bangladesh's advocacy through the Take Back the Tech Bangladesh[14] campaign. Tack Back the Tech Bangladesh aimed to increase awareness of cybersecurity issues, in particular the intersection of cybersecurity and violence against women. The Kenyan case study examined the Kenya ICT Action Network's engagement with the development of a cybersecurity bill that could potentially threaten privacy and cybersecurity in Kenya. The South Korean case study focused on efforts by civil society, including APC member Jinbonet, to reform the state intelligence apparatus to provide greater protection for human rights.

Take Back the Tech Bangladesh, part of an annual global campaign against online gender-based violence implemented by APC Member Bytesforall Bangladesh, aimed to increase awareness around the increasing relevance of cybersecurity issues as more users, particularly women and youth, begin to access the internet in Bangladesh. These issues included online harassment, cybersecurity issues, privacy, cyberbullying, and threats to and violence and abuse against bloggers and sharers of internet content.

In this case, advocacy combined with existing state structures for dealing with cybersecurity helped integrate human rights concerns by looking at internet-mediated gender-based violence through a cybersecurity lens. This was achieved through a mixture of awareness raising (in the form of a campaign) and consultations with relevant stakeholders through workshops that

14. Take Back the Tech! is a collaborative campaign to reclaim information and communication technology (ICT) to end gender-based violence initiated by APC. Many APC members, including Bytesforall Bangladesh, run localised Take Back the Tech! campaigns every year. For more information visit https://www.takebackthetech.net

aimed to both point towards solutions and amplify marginalised voices in cybersecurity debates. The workshops, along with consultations with policy makers, were the main mechanisms used by the Take Back the Tech Bangladesh campaign for advocacy and outreach. The workshops and consultations helped to advocate for better policies and practices that put cybersecurity on the rights track, with a particular focus on the rights of women and marginalised communities. The campaign thus also aimed to have, and had, direct influence on policy makers.

The Bangladesh case study was not just a campaign aimed at increasing awareness about new cybersecurity issues, but was also a multistakeholder campaign aimed at identifying, conceptualising and mapping new human rights issues arising from increased internet access. It points to the importance of listening to and understanding people's issues in order to conceptualise and frame advocacy in ways that are relevant to their needs and priorities.

The Bangladesh example also illustrated how civil society can effectively navigate a challenging landscape and identify sites of engagement with the government. They interacted with the government's Cyber Security Helpdesk around reports on cybersecurity, with policy makers on cybersecurity policy, and with techies on conceptualising how solutions can be developed and on mapping cybersecurity events.

The other two initiatives aimed to put cybersecurity on the human rights track through engagement with legislative processes rather than through awareness raising and advocacy.

The Kenyan case involved public and multistakeholder consultation and engagement around a draft cybersecurity bill that could

possibly threaten freedom of expression, the right to privacy, and internet access in Kenya. It looked at how the Kenya ICT Action Network (KICTANet), a self-described "multistakeholder think tank" and APC member organisation, engaged with a cybersecurity bill introduced in Kenya. The case study highlights challenges and best practices from KICTANet's engagement with the consultations around the bill.

The South Korean case study dealt with civil society engagement in the discussion and action around the review and reform of the laws affecting intelligence gathering and the South Korean intelligence agency, the National Intelligence Service. The Korean Progressive Network Jinbonet, an APC member organisation, was a key actor in this process. The case study highlights concerns and best practices that emerged from this experience of engaging with law reform and cybersecurity debates in a country in which there has been little engagement – until recently – by civil society with cybersecurity governance.

Whereas the Kenyan case study is of a policy development consultation process with KICTANet members raising objections to a bill in parliament, the South Korean case study looks at efforts to reform laws governing the National Intelligence Service, which is the custodian of state security. The means of reform is through proposing a bill into parliament that would try to reform the role of the National Intelligence Service, and take some of its authority for cybersecurity out of its domain and control.

The Kenyan and South Korean case studies have a common thread running through them of opposing the securitisation of internet issues – the narration of issues as existential security issues such that they are removed from the normal configuration of governance and brought onto the security agendas of states,

which has implications for how they are governed as well as potential human rights implications. They are in a sense also legislative and discursive practices of “de-securitisation” – bringing control over the discourse of security issues away from the state and attempting to put them under civilian or parliamentary control.

The Kenyan case looks at opposition from civil society to the securitisation of internet issues through proposed cybersecurity legislation that would have negative effects for privacy and freedom of expression. With public consultations, mandated by the Kenyan constitution, there is an opportunity to not only de-securitise but to mainstream human rights into the discourse and legislation around cybersecurity.

In the South Korean case, there was a civil society effort to introduce a draft bill that would bring some of the functions of the state security agency under civilian control. Jinbonet’s engagement with a task force comprising civil society and experts also aimed to de-securitise cybersecurity issues as well as to mainstream human rights into the discourse and legislation around cybersecurity. This was done by working on legislation to propose a bill to parliament (the National Assembly) rather than consulting around or opposing an already proposed bill.

Since South Korean civil society has little experience in formulating cybersecurity bills, the case study also represents a case of capacity building of civil society in engaging in legislative processes, as well as more broadly putting cybersecurity on the rights track. In addition to being a capacity building exercise, there were elements of awareness raising and advocacy. The South Korean case study also contributed to the building of

rights-respecting cybersecurity discourse in a situation in which most of the previous discourse had been state-centred.

The Bangladesh case is clearly an instance of civil society groups putting cybersecurity on the human rights track. Unlike the other cases, the Take Back the Tech Bangladesh campaign relied on securitisation of various security, social, internet and human rights issues and placing them onto a wider agenda. In the Bangladesh example, there was a need to securitise certain issues, and to put issues on the cybersecurity agenda, whereas in the other examples, there was a need to de-securitise certain issues by taking them off the national security agenda, and thus narrowing it.

Depending on context, both securitisation and de-securitisation are discursive practices that can be strategic in putting cyber-security on the human rights track.

5.1 Best practices for putting cybersecurity on the "rights track" identified from the three case studies

Both securitisation and de-securitisation can be useful in put-ting cybersecurity on the rights track – the best option will be dependent on the configurations of the societies and countries involved

In South Korea, current cybersecurity discourse and legislation concentrate cybersecurity functions under the state, especially its secretive and less transparent intelligence and state security arms. The case study involved a strategy of de-securitisation that aimed to give civil society and parliament more powers, voice and oversight over cybersecurity.

The Kenyan case study was a case also of de-securitisation, or more specifically, fighting back against the possibility of the spectre of encroaching securitisation through increased powers of the state over cybersecurity.

The Bangladesh case is an example of where securitisation of security issues can also put cybersecurity on the rights track. Gender-based violence and internet-mediated gender-based violence had not previously received enough attention from the state and were generally not seen as cybersecurity issues. Securitisation was a necessary strategy to put rights (especially those of women) on the cybersecurity and state agenda.

The case studies demonstrate that both widening the cybersecurity agenda (bringing issues onto the cybersecurity agenda) and narrowing the cybersecurity agenda (taking issues off the cybersecurity agenda) can be helpful in putting cybersecurity on the human rights track. Again, this is dependent on the societal and political context.

The South Korean case was a case of narrowing the cybersecurity agenda as it was an attempt to take powers and responsibilities away from the state and thus off the cybersecurity agenda through a particular focus on decreasing the powers of the National Intelligence Agency.

The Kenyan case was a case of fighting back against the widening of the cybersecurity agenda by taking more powers away from the state. It also involved some widening through putting issues like privacy on the cybersecurity agenda.

The Bangladesh case involved primarily a widening of the cybersecurity agenda by bringing gender-based violence and freedom

of expression onto the cybersecurity agenda in a country where gender-based violence perpetrated online and violence against bloggers and social media content creators are rife. Putting these issues onto the cybersecurity agenda helped to capture the attention and focus of the state.

Awareness raising is fundamental

All cases involved raising awareness about cybersecurity in order to put cybersecurity on the human rights track. This can be achieved through various means. In Bangladesh it was achieved through campaigns, workshops and multistakeholder consultation. In South Korea it was achieved through the act of bringing together civil society and experts to formulate a cyber-security bill, as well as though the societal awareness that would result from the actual bill being introduced into parliament, thus attracting the attention of policy makers, the media, and by proxy, society as a whole. The Kenyan case created awareness through engagement by a multistakeholder organisation, KICTANet, and through the use of public consultation mandated by the constitution.

Capacity building is a good entry point for multistakeholder networking

The workshops convened in Bangladesh helped to build the capacity of different stakeholder groups to talk about their issues in cybersecurity terms and to engage in advocacy.

KICTANet is an example of a multistakeholder group that has had its capacity built over the years through its mailing list as well as through public consultations bringing different stake-holder groups together.

Korean civil society and academics have previously not had much experience in engaging in cybersecurity policy formulation. Bringing together experts and civil society groups helped to build civil society's capacity to understand cybersecurity issues, to formulate cybersecurity policy and engage with legislatures.

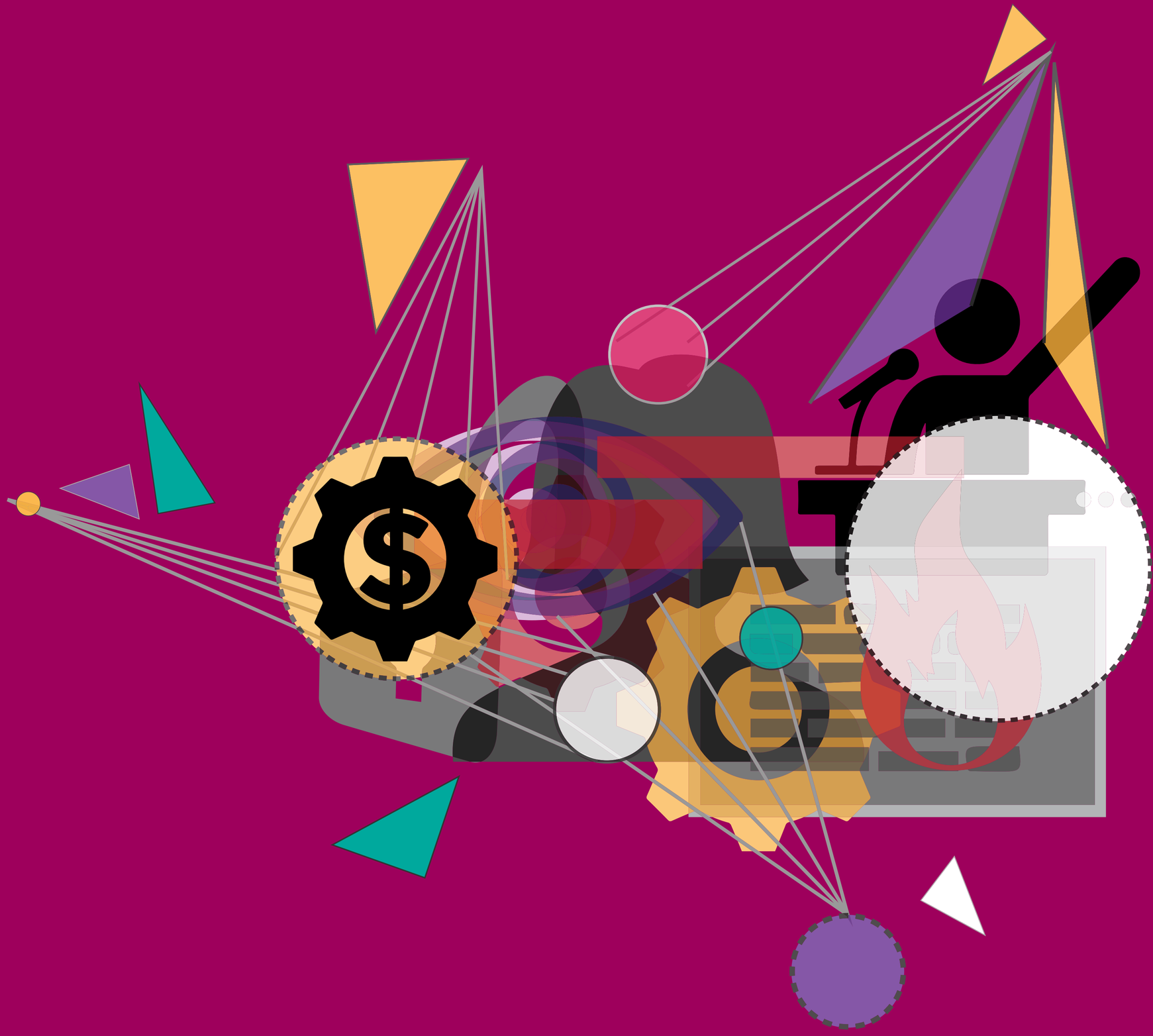
Listening to and amplifying the voices of the marginalised/affected communities is key

One of strategies used in the Bangladesh case study relied on capturing and amplifying the voices of marginalised groups (in particular women and social media activists) in society. The workshops capturing inputs, strategies and opinions from marginalised groups enabled "experts", activists and policy makers to gain insights into cybersecurity by listening to marginalised voices. These voices were then amplified through their representation in multistakeholder forums that included policy makers and through the Take Back the Tech campaign drawing attention to groups who are often not taken into account. Listening to the voices, experiences and perspectives of people who do not feel safe or secure online shifted the perception of cybersecurity and safety of experts and policy makers.

Multistakeholder approaches to cybersecurity are effective

All of the case studies point to the importance of the multistakeholder approach. They all involved as actors a combination of civil society (NGOs, activists and community groups), the research and technical community ("experts"), and policy makers (politicians and parliamentarians), as well as internet users in general.

“Gender, politics, economics, culture [and] language, all have an influence in cybersecurity, in the probability of risks, in the implications and perceptions of effects, [and] on the harm that can cause.”



APPENDIX 1: DETAILED REPORT ON THE SURVEY WITH APC MEMBERS

A. Introduction

APC conducted a survey of its members and close partners as part of the “Putting cybersecurity on the rights track” project. The respondents to the survey were APC members, partners and friends from countries around the world.

B. Overview of respondents

A total of 22 responses came from Australia, Cameroon, Chile, the Gambia, India, Kenya, Myanmar, Nigeria, the Republic of Korea (South Korea), South Africa, Spain, Uganda and Venezuela. Respondents lived and worked in 17 different cities: Abuja (Nigeria), Barcelona (Spain), Brisbane (Australia), Cape Town (South Africa), Mthatha (South Africa), Cumaná (Venezuela), Kampala (Uganda), Erode (India), Kanifing Municipality (The Gambia), Kano (Nigeria), Lagos (Nigeria), Nairobi (Kenya), Newrybar (Australia), Santiago (Chile), Seoul (South Korea), Yangon (Myanmar), and Yaounde (Cameroon).

They came from the following organisations: Asia Pacific Network Information Centre (APNIC), the Centre for Information Technology and Development (CITAD), Derechos Digitales, the Gambia YMCA Computer Training Centre and Digital Studio, the Global Forum on Cyber Expertise (GFCE), Internet Society India, the Kenya ICT Action Network (KICTANet), Korean Progressive Network Jinbonet, Myanmar ICT for Development Organization (MIDO), Nameshop, Net Freedom Pioneers, the Nigerian Federal Ministry of Communications, Pangea, Paradigm Initiative, PROTEGE QV, Right2Know Campaign, the Technical University of Catalonia, TICsLegal, Transworld Africa Limited, Woman of Uganda Network (WOUGNET), Wikimedia South Africa, and Zenzeleni Networks.

Their vocations or positions included directors, executive directors, researchers/analysts, business owners, advisors, network administrators, volunteers, professors, consultants, computer analysts, and the self-employed.

Below is a summary of responses to the different thematic areas covered by survey questions.

C. The relevance of gender to cybersecurity

When respondents were asked if they felt that gender mattered to cybersecurity, responses varied. One respondent, identifying as male, stated: “Gender, politics, economics, culture, [and] language, all have an influence in cybersecurity, in the probability of risks, in the implications and perceptions of effects, [and] on the harm that can cause.”

Another respondent, a woman, answered: “Definitely, gender issues are under-represented in cybersecurity. Women confront different threats online not usually considered in cybersecurity design.”

One male respondent felt that gender did not matter: “No – any relevance is not pertaining to cybersecurity directly – cybersecurity is about access control and security of electronics and technology. The motives for tampering with those, and demographics of those who do, might involve gender, but the means do not.”

Another male respondent felt that gender was relevant, “because I am more assertive in my online environment,” suggesting that men feel more secure online, and that it is easier for men to express strong views and opinions online than it is for women.

D. Defining cybersecurity

Respondents offered a variety of definitions of cybersecurity, which ranged from fairly narrow, to very broad. None of the definitions linked cybersecurity to national security.

Broad, overarching definitions included:

- "Cybersecurity is a collection of measures to preserve the integrity of cyberspace, measures in right proportion, to ensure that the space is not abused, that the space does not become dangerous to the global economy, the global society."
- "Cybersecurity is everything related to privacy and security as it pertains to electronic communications and data – including the means to safeguard it, respond to events as well as awareness of the issues. Many people do not realize how technology is fundamentally different from other things they encounter in the real world, and as such are not aware of the issues – of something commonplace, such as password reuse."
- "Cybersecurity is to maintain integrity and stability of data and networks from various internal and external threats."
- "Cybersecurity is protecting yourself online, data protection, and privacy."
- "From a technical perspective cybersecurity can be defined under the CIA model – Confidentiality, Integrity, Availability. In addition, cybersecurity includes the necessary state of trust, both real and perceived, in the Internet, networks, applications, and devices that provides sufficient confidence in users for their continued use."

Four definitions emphasised capacity and control on the part of the individual user:

- "Cybersecurity is knowing how to navigate the Internet safely."

- “Cybersecurity is my ability to maintain reliable private communications online.”
- “Cybersecurity is the extent to which an individual remains safe online in the face of negative consequences of the digital world e.g. digital theft, fraud, sexual harassment, misogynistic practices etc. The concept also connotes safety, protection and control of online platforms in ways that is beneficial to all.”
- “Cybersecurity is for me is the way I can use digital tools without being afraid that my data could be [intercepted] or used by someone else.”

Several cited the security of people along with the security of systems:

- “Cybersecurity is a topic related to the protection of digital devices, and people in the digital world. It relates to safety, prevention that nothing bad happens.”
- “Cybersecurity is the protection of the internet as to ensure that people are safe when they use it and that no harm comes to them because of the way other people are using it.”
- “Cybersecurity is the protection of the confidentiality, integrity and availability of information with the end of protecting people both online and offline. This measures also apply to the underlining infrastructure in which the information is processed, and can be of policy, technical or educational nature.”

Narrower definitions include one focused on online data only, one focused on online information and transactions, and one on internet systems:

- “Cybersecurity is protecting the data that is online.”
- “Cybersecurity is the means of ensuring integrity of information and transactions on the internet.”
- “Cybersecurity is safeguarding internet systems from compromise.”

E. Cybersecurity and human rights

E.1 Relationship between human rights and cybersecurity

Respondents were asked what the relationship was between human rights and cybersecurity.

One said there is clearly a relationship because of the extent to which the personal has become digital:

> Our personal life has a digital part. Our recorded files, images, messages, history, interactions are [increasingly] in digital form. Our memories are also linked to digital experiences. Our experiences, good or bad too and all have a "cyber component". The digital world surrounds us more and more, therefore our personal security [increasingly] depends on cybersecurity. Feeling safe now depends on the digital. Everyone has experience [of] the bad feelings of the aggression of getting a message or call in the middle of the night that your credit card or bank account has been stolen, your account, computer or mobile has been hacked, someone has published a personal photo about you, or said something bad in Twitter, etc.

Another responded talked about the dual nature of the link. One the one hand, threats can impact on the right to access, or the right to privacy. But on the other hand, measures taken to increase cybersecurity can themselves infringe on rights:

> Threat[s] to data and network[s] would infringe on the right to access by shutting down networks, and [infringe] on the right to privacy by leaking personal data or altering confidential information. [On the other hand] measures [towards] cyber-

> security could infringe human rights by surveilling networks and devices, or by retaining and [harvesting] personal data for investigation.

Surveillance was also mentioned by another respondent, who further pointed out that rights advocates are to some extent naïve in how they perceive, and use, technology:

> Electronic communications and media can be used to track, intimidate and manipulate people. Human rights is a political issue and as such, technology is just another tool in the political arsenal. People who advocate for the rights of the technologically excluded, might not be aware of these new weapons that can be pointed at them, to silence them or paint them in an unfaithful light.

Another pointed out how “cybersecurity is often used as an excuse by governments to disproportionately increase their surveillance capacity.”

One respondent noted that both cybersecurity and human rights rely on two very fundamental concepts or principles: privacy and anonymity. This is an interesting comment, and supports APC’s position that cybersecurity is a human rights issue and that respect for rights, such as the right to being anonymous online and the right to privacy, contributes to cybersecurity and affirms human rights.

Someone else put this very succinctly: “Cybersecurity protects human rights.” Another affirmed this by stating: “Cybersecurity gives more confidence to users or protects their data, and by doing so protect[s] their rights.”

Another respondent described the link between human rights and cybersecurity as follows:

> At one level, cybersecurity is the extension of our rights offline. At a more practical level, misuse of cybersecurity can lead to derogation our rights to privacy, confidentiality as well as to dignity, and in extreme cases to the right to life.

Someone responded from a broad view of cyberspace:

> Cyberspace is a means by which people interact, communicate, develop socially and economically. To be able to exercise their human rights in the digital environment people's interactions online must be secure of outside intervention, both from governments and private companies.

Another illustrated the relationship through an example:

> Let us say a hospital stores information on the health status of its patients, including what they suffer from. Then a malicious attacker gets access to that data and publishes it in a widely accessible manner. Have the patient's human rights been violated through the exposure? The patients will feel insecure, exposed and vulnerable. That is an example of the relationship between human rights and cybersecurity. An example of this breach happened in Singapore.

One person summed it up concisely: "Deprivation of my cybersecurity denies me the ability to defend human rights."

E.2 What human rights do you see threatened by cyber insecurity?

Respondents highlighted the following rights. It is important to note that they did not have a drop down list of fundamental rights described in formal or legal language.

Seeking, accessing and sharing information

“The right to citizens participation in governance. Cybersecurity concern is leading to closure and shutdown of the internet, thus making it difficult for people to receive and share information. Without this, cultural expression is hampered. Again, without information, citizens are unable to make informed decision, and are unable to participate meaningfully in the governance of their countries.”

Privacy and freedom of expression

“Right to privacy or data protection by mass data leakage, by seizure and search, and surveillance by investigative and intelligence agencies.”

“Privacy mainly, and by extension freedom of expression, when one suspects he is under surveillance.”

“Privacy and data protection.”

Access to the internet

“Cyberattacks that bring down networks interferes with people’s ability to access the internet.”

Human rights in general

Two respondents felt that all human rights are threatened. One elaborated:

> Platform operators filter who sees our messages, infringing on our right to free speech. Knowledge about disease can be life threatening or life changing – privacy, freedom of association, education, forced labour – all of these things can be undermined by technology, and technology that can affect something for the positive necessarily affects it to the negative if it does not function transparently and as would be expected by the non-technical.

The other mentioned the impact on rights of cybercrimes such as phishing and identity theft.

F. Threats related to cybersecurity or insecurity

Respondents were asked to identify three different types of cybersecurity threats: threats to them personally, threats to their organisations and the people they work with, and threats to broader civil society. There was a lot of overlap between what respondents saw as threats to them personally, to their organisations and to civil society in general, and it was difficult to document responses in a way that usefully categorises the threats in the table below, which contains a lot of repeated content.

One respondent remarked that what is unique to threats in cyberspace is that the tools and means of attack are “equally available to small groups of criminals and extremists.” Sever-

al pointed out that surveillance, one of the most commonly felt threats, is perpetrated by state institutions, such as law enforcement and intelligence agencies, as well as by companies. Sometimes surveillance is backed up by regulation, at times it is visible, often it is not. One respondent suggested that internet service providers are often complicit with state-driven surveillance. The inability to trust that one's communications are secure and private undermines civil society's effective use of the internet.

F.1 Types of threats and their targets

Threats to you personally	Threats to your organisation and those you work with	Threats to civil society

Surveillance
• In different forms from different sources including states, platforms, intelligence agencies. Sometimes this is through regulatory measures, and sometimes it is "unofficial".
• From law enforcement and intelligence agencies.
• Surveillance through regulation of the internet.
 	
Lack of control over technology one uses and of one's own data
• Lack of control over personal data being collected by different actors, possibility of use of metadata to intrude on privacy of individuals, governments reading cybersecurity to deploy electronic surveillance on ordinary people, the possibility that it may harm democracy.
• Dependence on email providers who are part of the military-industrial complex. Primary address is Gmail, secondary is academic but the academy has outsourced the service to Microsoft. Following a particularly intense bout of Wikileaks-related communication on the [organisation's] list, I was locked out of my Gmail account for some hours (by being told my password was wrong, and when I tried the procedure for changing passwords, the recovery code failed to come to my phone as promised. However service resumed with the old password at exactly midnight.
 	
Physical and psychological threats
• Seize and search of my device by law enforcement agencies.
• Threats to the security of my environment with the intention to cause harm or affect my personal integrity, emotional state, etc.
• Attacks on critical infrastructure functioning.
	Surveillance
	• From law enforcement and intelligence agencies
	• Loss of the right to privacy
	• Government surveillance
	• Metadata retention
	• Private surveillance and hacking.
	
	Physical and psychological threats
	• Attacks to critical infrastructure functioning.
	• Coordinated attacks against vulnerable groups' online presence.
	• Seize and search of our server by law enforcement agencies.
	• Hacking of or attacking to our servers.
	• Equivalent to the list before, but applied to my technical, community service and political activity, that can prevent, limit, or change my freedom, actions, effectiveness, reputation, etc.
	• Cybersecurity is not something I study, and is not something that is top of mind - I know how to keep a computer secure, and how many ways there are to break that security.
	• The ability of people, especially women and girls to feel safe online the ability to use the internet without government shutdown the differential in terms of both accessibility and affordability that is driving digital marginalization and exclusion of certain groups of people.
	• To my work:
	  o Collecting data and personal information.
	  o Surveillance through regulation tools.
	• To those we work with:
	  o Non respect to privacy
	  o Collecting data and personal information.
		Surveillance
		• Data collection, wiretapping, location tracking, hacking etc.) from law enforcement and intelligence agencies
		• Government surveillance
		• Metadata retention
		• Private surveillance and hacking.
		
		Physical and psychological threats
		• Harassment
		• Attacks to critical infrastructure functioning
		• Coordinated attacks against vulnerable groups online presence
		• DDoS attacks
		• Seize and search of devices by law enforcement agencies
		• Exploitation in many forms, control in different degrees (from the subtle of ads, to the strong of physical abuse) all supported by digital components.
		• Over-dramatization of cyber-insecurity by governments to want have undue control over how people access and use the internet.
		• Everything is digital or has a digital component nowadays, therefore anything can be affected, controlled to affect, determine, prevent, coerce, suppress or transform our collective perceptions and actions.
		• Civil society is dependent on technology to get through the day - more so in urban centers than in rural areas. A system that experiences down time due to a breach can result in wasted time or lost lives in a worst case. Moreover, a government, ISP or platform operator, with undue visibility - or unequal visibility of a data set, might make economical or political decisions or interventions to achieve a goal that will benefit a few at the expense of a many.

Threats to you personally	Threats to your organisation and those you work with	Threats to civil society

Hacking/exposure of personal details (cybercrime)
• Threats resulting from cybercrime that can lead to loss of data, financial losses and identify theft:
  o Phishing attacks
  o Malware attacks
  o Website hijacking
  o Identity theft
  o Viruses.
• Hacking of my personal account (by various criminals).
• Access and disclosure against my will of personal details, files, bank account, opinions, details in general.
 	
Blackmail, manipulation and/or intimidation
• Taking advantage of detailed knowledge about me and my activities to have an influence or power to limit my freedom, choice, emotional state, options, activity.
• As a systems/network administrator, I may be caught off guard, or manipulated by power structures in my or another organization, to give access to someone with a nefarious purpose, explicitly or through my own neglect. I may be kept busy with something else while something that should not happen takes place under my watch. I may not have control over parts of the networks that I am tasked with protecting. I may be responsible for more networks and more uninformed people running these networks, than I am capable of supporting.
 	
Other
• Misinformation.
• Military use of cybersecurity technologies, not only for prevention of attacks but also for cross-border offence in some cases.
• Security measures put in place counter productively creating newer threats.
• Disproportionate measures altering the way we live our lives.
	Threats from security providers and services
	• Security only exists in layers, and some of them are organizational and social, while most of them are purely technical. Someone, say an “auditor” or a “supplier” might interfere with a system that I am tasked with maintaining, in order to undermine my ability to achieve a certain scale or uptake of a service run with a certain economical or political motive. Communications can be blocked or manipulated such that those in my organization are undermined, or had undue influence.
	
	Hacking/exposure of personal details/information (cybercrime)
	• Phishing attacks
	• Malware attacks
	• Website hijacking
	• Personal data leaks
	• Viruses
	• Stolen data
	• Identity theft and fraudulent activities
	• My computer and phone are no longer my own.
	• Most of my data is inevitably on the cloud.
	• My Internet connection is not secure.
	• Someone wrongly decides to add one of my email addresses to the spam list, I don’t know that, and even when I find out, there is very little that I can do to remove the wrong entry. Same is true of a tweet or Facebook post not added to the hashtag stream or post feed.
		Hacking/exposure of personal details/information (cybercrime)
		• Personal data leaks
		• Phishing
		• Viruses
		• Data theft.
		
		Loss of civil liberties
		• Various cybersecurity measures, seen and unseen, though necessary to some degree, are often decided without consultation or due examination and result in the erosion of civil liberties.

F.2 National, regional and international threats

National threats	Regional threats	International threats
Mass data leakage by insider of data controller or hacking, which lead to fishing and identity theft. Hacking or attacking of critical resources from hackers (some of them may be from north Korea) Hacking of accounts, specially with economic and privacy implications (bank account, credit card, personal email or social info, tax info, health), impersonation. Monitoring of communications (voice and Internet), not only as a result of a legal request, but also by massive or targeted surveillance by the police and specially secret services. Monitoring of private actors of infringements such as copyright or software licenses. Profiling of citizens as they use private or public transportation, and other similar profiling activities from widespread data collection (faces, license plates, etc.). Attacks to infrastructures.	The above plus perhaps additional surveillance related to the political situation of the independence movement, which has brought probably covert mass surveillance, DDoS and hacking attacks, etc.-	Using hacking tool for surveillance by investigative and intelligence agencies. Mass surveillance by intelligence agencies. Cyber attack or hacking between countries. Too many to list, and not different from the previous.
I do not think cyber security discriminates based on country - but illiteracy and low technical knowledge might be a bigger problem here than elsewhere.	I do not think cyber security discriminates based on country - but illiteracy and low technical knowledge might be a bigger problem here than elsewhere.	Opaque and proprietary systems, that can not be examined - and proprietors of those who can not be held to account.
Lack of data protection mechanisms, hate speech online, gender-violence online.	Lack of data protection mechanisms, hate speech online, gender-violence online.	Data protection and privacy issues
We have rogue police and intelligence staff and adjacent private operators (usually ex-cops/agents) who access cellular metadata at will due to the requirement that we register every SIM.	Some countries have internet shutdowns at politically tense times. In SA. we had a jamming attempt within the house of Parliament a few years ago but it was cut short by the united outrage of opposition parties.	The military-industrial complex. All that Snowden et al revealed.
Same as mentioned in previous section	The same as above, including expansive state funded attacks	Phishing attacks Hacking attacks DDoS attacks Malware infections.
1. Lack of updated data protection regulation 2. Lack of updated cyber crime regulation 3. Phishing 4. Personal data leaks 5. Government and private surveillance and hacking 6. Coordinated attacks from foreign actors to financial system. 7. Surveillance through regulation tools	1. Government and private surveillance and hacking 2. Lack of protection for encryption 3. Software backdoors 4. Lack of updated data protection regulation. 5. Surveillance through regulation tools	1. Government and private surveillance and hacking 2. Lack of protection for encryption 3. Software backdoors 4. Personal data leaks 5. Phishing 6. Attacks to critical infrastructure functioning 7. Coordinated attacks against vulnerable groups online presence 8. Metadata retention. 9. Privacy data protection

Same as above	Online fraud targeting financial institutions, hacking, spying or cyber espionage	Rights to personal privacy and data protection
1. Unsecured phones, operating systems. 2. Lack of knowledge to judge what and what not to trust on the Internet.	1. First of the global threats are identified by answering the questions "how secure is security?" and "Whom does Security secure?" 2. Distinct from (1) above, the international threats concern the helplessness concerning the inevitable vulnerability of physical spaces, infrastructure and lives in a world of real, perceived and propagandised historical and some current injustices by one nation to another, by one culture to another, in both directions, often as a crossflow	1-3; 4-15; 18-21; 27, 29-30 some indirectly.

G. Mapping national and regional cybersecurity landscapes

Eleven APC members from nine countries (two each from two countries) completed a national and regional cybersecurity mapping exercise which asked them to identify related institutions and actors and processes. In Africa there were responses from Cameroon, the Gambia, Nigeria, South Africa and Uganda; in Asia from India and South Korea; and in Latin America from Chile.

G.1 Korea

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
National Security Office under Blue House National Intelligence Service of Korea Ministry of Science and ICT Korean Internet & Security Agency (KISA) National Assembly Intelligence Committee Technology Research Institute for National Security (NSR) Academia, such as Korea University Graduate School of Information Security	No response	Officially National Security Office under Blue House is responsible for national cybersecurity strategy and coordination, But I guess National Intelligence Service of Korea would do that in practice.	National Intelligence Service of Korea has been responsible for national cybersecurity policy and cybersecurity of public network. But NIS has been infamous for political intervention and inspection against civilian which infringe human rights severely, so has been demanded to reform its mission, authority and structure. There is not supervisory mechanism to monitor the NIS.	Strongly disagree There is no public consultation for national cyber security strategy. Even the intelligence committee of the National Assembly is very closed.	National Cyber Safety Management Regulation (presidential decree) ACT ON THE PROTECTION OF INFORMATION AND COMMUNICATIONS INFRASTRUCTURE, which is for cyber security of critical infrastructure in public and private sector ACT ON PROMOTION OF UTILIZATION OF INFORMATION AND COMMUNICATIONS NETWORK, which includes provisions for cyber security in information and communication network ELECTRONIC GOVERNMENT ACT, which includes provisions for cyber security of electronic government system PROTECTION OF COMMUNICATIONS SECRETS ACT, which deals with wiretapping and access to meta data by investigative and intelligence agencies. ACT ON ANTI-TERRORISM FOR THE PROTECTION OF CITIZENS AND PUBLIC SECURITY	National Intelligence Service of Korea has been responsible for national cyber security policy and cyber security of public network. But NIS has been infamous for political intervention and inspection against civilian which infringe human rights severely, so has been demanded to reform its mission, authority and structure. There is no supervisory mechanism to monitor the NIS.

G.2 Spain

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
Formal: secret services, public cybersecurity agencies (e.g. CNI from the Spanish gov, the Security office of the Catalan government as well other regions, data protection agencies, the academic Red.es, CERTs, EU), police (specialised groups on cybercrime), private operators (telecoms, cloud, services). Civil society and informal: such as NGOs doing campaigns such as nodo50, x-net, Pangea among others.	Governmental organisations on the public sphere (e.g. national and regional governments, data protection agencies, EU), private organizations in the private sector (every large service provider)		Hard to explain, not directly	Disagree	Yes, passed but not practically enacted.	Several actions by police and secret services have that effect, sometimes from deliberate action (interest to cause problems or condition some persons or groups), sometimes from inaction, others from incompetence on lack of understanding (e.g. blocking, disclosing, creating false information).

G.3. South Africa

There were two respondents from South Africa.

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
First respondent: Our government has a cybersecurity task force - but it is trying to replicate things that have already been perfected by other institutions, poorly. We have internet service providers' associations, and ISOC chapters - who barely manage to scratch the surface toward doing anything meaningful - with just a bit of the right incentive or motivation, they can be a lot more practical. All previous efforts that I am aware of have been meaningless and short lived efforts by commercial bodies to extract revenues. *Second respondent:* Rogue police and intelligence	*First respondent:* The large ISPs. They engage with people using technology the most, and a message from them might be more relevant - they lack incentive and skills to do anything meaningful. *Second respondent:* Right2Know, Research Internet Africa, ISOC, community networks.	*First respondent:* I don't know much about these, and I am skeptical of their usefulness in this. For every regulation there is an equal and opposite loophole. This is not only true of regulations, but it happens in cybersecurity in real time. There are however mitigation tactics that are exponentially more effective than others - for example rate limiting makes technology act more like real world things. A firewall can protect insecure items much like a front door can protect things inside a house. I doubt that complex technical matters are explained simply enough to lawmakers and politicians, and if anyone can it would be us - there are only so many types of vulnerabilities, and each can be articulated in a simple, universal metaphor, relevant to the culture or context, putting the risk and the effectiveness and sacrifice needed for an effective mitigation, in context. *Second respondent:* We have a moronic Film Control Board which railroaded impractically megalomaniacal legislation that could enable censorship, plus the "normal" surveillance already mentioned above	*First respondent:* Isn't all of government tasked with protecting our human rights? They all use technology. But each department needs its own independent "cybersecurity" and "technology" department, because if they all use the same one, that is a risk - it is like having a soldier commanded by some outside independent army, in each body of government, ready to strike at the command of another body. *Second respondent:* Police ("Crime Intelligence"), State Security Agency, Film & Publications Board all have surveillance capacity and ability to censor.	*First respondent:* Strongly disagree Comments: Political participation in our country is low - especially so in technology. Very few people know how our processes work, and fewer still can afford to take the time to participate - most participation comes from large groups with vested interests. Outreach to educate people on the workings of technology, and grants to promote participation, can improve things. *Second respondent:* Disagree Comments: We have a charade of public participation but in the end power is served.	*First respondent:* I am not on top of this, but I have seen meetings about drafts and government things, at tech conferences. *Second respondent:* Yes, with more in the pipeline.	*First respondent:* Not that I'm aware of. How would one notice? Would someone who is incompetent at raising the issues practically count?

G.4 Nigeria

There were two respondents from Nigeria

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
First respondent: • Office of the National Security Adviser • The Economic and Financial Crimes Commission • The State Security Services • Office of the Attorney General • The National Information Technology Development Agency • 16. National Commission for Identity • Nigeria Communications Commission *Second respondent:* • National Information Technology Development Agency • Nigerian Communications Commission	*First respondent:* The National Assembly Committee on Cybercrime and its Annual Conference The Cybercrime Experts and its Annual Conference. *Second respondent:* • Paradigm Initiative • CcHub • Digital Rights and Inclusion Forum	*First respondent:* The enactment of the Cybercrime law *Second respondent:* National Information Technology Development Agency and Nigerian Communi-cations Commission (NCC)	*First respondent:* All of previously mentioned organisations. Their action impact on space for the flourishing of human rights. Some of these organizations want tighter government control of the internet. Some have cause the arrest and detention of bloggers and journalists for a purported cybercrimes. *Second respondent:* Paradigm Initiative and CcHub are civil society organizations working to secure citizens' cybersecurity.	*First respondent:* Disagree *Second respondent:* Disagree	*First respondent:* Yes *Second respondent:* Cybercrime Act 2015	*First respondent:* They interpret any view that is critical of government or government officials as cybercrime. Second respondent *Second respondent:* The NCC sometimes passes policy which undermines human rights in the digital age.

G.5 Chile

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
• Government CSIRT • Ministry of Ministry of Domestic Affairs • Ministry of Defence • Inter ministerial cybersecurity committee • Cybersecurity Alliance • Secretariat of Telecommunications • Derechos Digitales • Tech industry	• Ministry of Domestic Affairs • Cybersecurity chief • Inter-ministerial cybersecurity committee • National Congress	National Congress, Inter ministerial cyber-security committee (executive branch), Ministry of Domestic Affairs	All decision-making structures, since cybersecurity discussions and policies always involve human rights.	Disagree Comments: The National Cybersecurity Strategy was drafted in a multi-stakeholder manner, but since the new government took over, decisions have been made in a less open and participatory way, giving excessive participation to industry and not enough room for civil society.	A new law was passed recently creating the cybersecurity awareness month (October), we are also currently discussing the modification of the cybercrime law to implement the Budapest Convention.	The police and the investigation police tend to push to extend the period of data retention and reduce the rights of people to due process in cybercrime legislation. They are increasingly implementing the use of surveillance software in their investigations without specific oversight or regulations regarding those uses.

G.6 Cameroon

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
ANTIC, www.anti.cm ART, www.art.cm Police structures	ANTIC, www.anti.cm ART, www.art.cm	ANTIC, www.anti.cm ART, www.art.cm police structures	National Commission on Human rights ANTIC, www.anti.cm ART, www.art.cm	Strongly disagree Comments: Only the state and his agencies are involve on the issues.	Yes: Loi_2010-012_ cybersecurite_cyber-criminalite	Yes. Many actors cited, are not independent and so can not be neutral.

G.7 The Gambia

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
The Regulatory Authority. ICT Line Ministry and The IT Association	National Internet Governance Forum	At the ICT Ministry	The ICT Line Ministry Working with Our Ministry of Justice	Strongly disagree. Comments: It is discussed within our national IGF steering committee.	NOT YET	

G.8 Uganda

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
Uganda Communication Commission, National Information Technology Authority, Computer Emergency Response Team, Uganda Registration Services Bureau, Telecom Companies and security establishment	FIFA regularly convened by CIPESA	1. UCC; 2. NITA-U; 3.CERT; 4.security establishment	NITA -U and Ministry of ICT, CIPESA, Women of Uganda Network, etc.	Disagree Comments: Normally this are done by government actors and those in security	YES	The institution of parliament which is used as a patronage tool in Uganda, those in security establishment who likes to securitise cyber security issues etc.

G.9 India

Key cybersecurity actors	Organisations relevant to cybersecurity	Decision-making structures	Organisations relevant to human rights	"Cybersecurity decisions are made in a multi-stakeholder manner"	Recent cybersecurity legislation	National actors undermining human rights
CERT, cyber security divisions of provincial (state) police, central (federal) bureau of investigations, Ministry of Home, a few quasi government agencies, NGOs, private contractors	Closed Government and Law Order Agency meetings and closed deliberations largely determine cyber security measures in India at present. In India and elsewhere.			Strongly disagree Comments: Normally this are done by government actors and those in security	YES	The institution of parliament which is used as a patronage tool in Uganda, those in security establishment who likes to securitise cyber security issues etc..

H. Research agenda

Respondents were asked what cybersecurity concepts and issues they would like to see unpacked and investigated as part of a longer-term APC research agenda. Responses included:

- Effects of mass surveillance on different social groups.
- Unlawful actions by secret services, police, and private actors.
- The cybersecurity of social media platforms (run by private organisations).
- The security and privacy of software and tools.
- Economic and other forms of crime.
- Effects on critical infrastructures.
- Cybercrime in general.
- Abuse of vulnerable groups.
- Explaining cybersecurity simply.
- The relevancy of policy – other than governments who want skeleton keys to all our digital lives, or want to keep ISPs and platforms from the same. State-sponsored attacks.
- The gravity of certain security threats and understand if and why such grave threats do not have anything other than solutions on the present track, which to my uneducated mind, appears counter-extreme, or at least disproportionate, and in some cases unjust towards a good section of those inevitably classed together with the offenders. If there is even a minor possibility of resolving issues by an alternate master plan and by alternate strategies, I wish to explore and contribute.
- The nexus between human rights and cybersecurity, how cybersecurity is being used by governments to derogate human rights.
- The role of state-sponsored hackers.
- Connection between cybersecurity and gender.
- How can multistakeholder participation help developing countries create better implementation of national cybersecurity policies.
- Model of founding multistakeholder cybersecurity initiatives in developing countries.
- Cybersecurity protecting human rights.
- How cybersecurity issues operate across different regions – what the commonalities and differences are.
- Personal data protection.
- Collaboration by global civil society to maintain cybersecurity.
- Cyberoperations and the application of humanitarian law to cyberspace.
- Technical aspects of cyber security – critical network infrastructures, etc.
- Actual and potential contribution of community networks
- Cyber war or conflict between nations.

I. Respondents' interest in further work on "putting cybersecurity on the rights track"

Respondents were asked if they were interested in participating in APC's work on human rights-based approaches to cybersecurity, and, if so, how.

All said yes. Many said they were interested in research, rights activism, communications and outreach, and awareness raising. Some said they felt they lacked knowledge and expertise in the area and there is a definite interest in capacity-building opportunities. Several said they would like to collaborate with others in the network and share experiences. Most said they would like to participate in APC-initiated events and projects. One emphasised interest in playing an advocacy role:

> Absolutely by playing advocacy at national, regional and international level. I am also available to support APC in any way possible. I am also concerned about the primacy of state actors regarding cybersecurity issues and the fact that anything can be securitised by actors of the state as security or cybersecurity issues. I need practical technical skills to help debunk, advocate and engage actors around these aspects.

PUTTING CYBERSECURITY ON THE RIGHTS TRACK

December 2020
ISBN 978-92-95113-37-4
APC-202012-GAPS-R-EN-DIGITAL-327