APC POLICY EXPLAINERS

A HUMAN RIGHTS-BASED APPROACH TO CYBERSECURITY

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper

Definition

The problem

The change we want to see

How APC works on this issue

Regional implications

Where is the discussion taking place?

Some spaces and institutions to engage with

Read more

DEFINITION

A human rights-based approach to cybersecurity means 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 an approach is systematic, meaning that it addresses the technological, social and legal aspects together, and does not differentiate between national security interests and the security of the global internet.

THE PROBLEM

People, in particular human rights defenders (HRDs), groups that are subject to intersecting discrimination and marginalisation, and journalists, rely on the internet and its availability, integrity and confidentiality to exercise their human rights. If the internet is not secure, then their ability to exercise their rights can be threatened, and in extreme cases, their personal security.

For example, weakened encryption (through backdoors to software and devices) can make it easier for malicious hackers to gain access to people's personal communications and metadata, which can lead to journalists' sources being revealed, HRDs (and their networks) being targeted by governments, and a person in an abusive relationship being blackmailed. It is important to ask who/what the security in cybersecurity stands for – often cybersecurity policies, like national security policies, define security in relation to the state, rather than the people (and the infrastructure needed).

Insecurity on the internet is real, and threats to cybersecurity can be human rights violations. Examples of this include the following:

- Threats to encryption and anonymity-enhancing technologies (both legal and practical) undermine freedom of expression, opinion and assembly and the right to privacy. Laws outlawing the use of these tools, countries blocking encrypted apps, proposals for backdoor access and arrests of digital security trainers pose threats to these rights.

- Targeted malware and ransomware with different motivations (financial, security-related, etc.) all pose risks to privacy (and related rights).
- Government hacking (to get access to data in other jurisdictions) also poses a risk to these rights.
- Exploitation of vulnerabilities makes the internet less secure for everyone.
- Confidentiality of information being compromised, whether through data breaches for financial gain, mass government surveillance or targeted attacks on HRDs or journalists, violates the right to privacy, among other rights.
- Distributed denial of service (DDoS) attacks, used by a variety of actors, render websites unavailable temporarily or indefinitely. These attacks have been aimed at activists and HRDs, among others.
- The denial of availability of information and its underlying infrastructure, in the form of network shutdowns, violates a wide range of rights, including by unduly restricting access to information and the ability of people to express themselves and peacefully assemble and associate, as well as enjoy a range of economic, social and cultural rights.

Most cybersecurity policy efforts tend to do little more than pay lip service to human rights. Many contain provisions that actually threaten or undermine rights, and cybersecurity is often pitted against human rights, i.e. you have to pick between privacy and security, or openness and vulnerability. This framing is misguided and counterproductive. Security is a human right. Rather than balancing rights against security, cybersecurity policies must provide security in a way that reinforces human rights.

THE CHANGE WE WANT TO SEE

A secure internet is best achieved through a rights-based approach and must centre on the security of users as opposed to the security of states. Cybersecurity practices, policies and strategies should place human rights at the centre and not treat them as inherently at odds with each other.

HOW APC WORKS ON THIS ISSUE

APC promotes a human rights-based approach to cybersecurity since humans are the ones impacted by cyberthreats, incidents and operations. We also apply a gender approach to cybersecurity, recognising that cyberthreats differentially affect groups in positions of marginalisation or vulnerability because of their sexual orientation or gender identity.

APC conducts research on this issue, and monitors policy development on this topic at global, regional and national level. We work collaboratively with our members, partners, other civil society organisations, academia and the tech community to advocate for the development of principles and norms to promote the idea of a rights-based approach to cybersecurity. APC also maps policies in its members' countries and regions. At the global, regional and national levels, APC advocates for more open and participatory cyberpolicy processes.

REGIONAL IMPLICATIONS

What happens in global cybersecurity discussions influences processes at the regional and national levels (and vice versa): global norms can have an important influence on what states do at the national and regional level. In order to be implemented, global norms on cybersecurity require policy and regulatory instruments, policies and frameworks. Increasingly, regional intergovernmental bodies are addressing cybersecurity, including the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN), the African Union and the European Union (EU).

WHERE IS THE DISCUSSION TAKING PLACE?

At the international level, cybersecurity has been debated at spaces such as the UN General Assembly First Committee and at the International Telecommunication Union (ITU).
In late 2018, the UN First Committee established two parallel processes to discuss responsible state behaviour in cyberspace – the UN Group of Governmental Experts (GGE) and the Open-ended Working Group (OEWG) (click here for an explainer on these processes). A number of reports by UN Human Rights Council Special Procedures also cover the issue of encryption and surveillance. The ITU carries out a number of activities aimed at "Building confidence and security in the use of ICTs", including through the development of the Global Cybersecurity Agenda (GCA) – as a framework for international cooperation in this area – and the Global Cybersecurity Index (GCI).

SOME SPACES AND INSTITUTIONS TO ENGAGE WITH

- Global Commission on the Stability of Cyberspace (GCSC)
- Freedom Online Coalition
- International Telecommunication Union (ITU)
- Organisation for Economic Co-operation and Development (OECD) Committee on Digital Economy Policy, for instance, through the Civil Society Information Society Advisory Council (CSISAC)
- Organization of American States (OAS) Inter-American Committee against Terrorism (CICTE)
- Internet Governance Forum Best Practice Forum on Cybersecurity
- UN Open-ended Working Group (OEWG)
- UN Group of Governmental Experts (GGE)

READ MORE

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

Briefing document: Cybersecurity policy and human rights

Recommendations for human rights-based approaches to cybersecurity

Towards a cyber security strategy for global civil society?

Why Gender Matters in International Cyber Security

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper

Lorem ipsum dolor sit amet, consectetut laoreet dolore magna aliqu