ITU Explainer: Cybersecurity

What is cybersecurity?

There are hundreds of different definitions of the term "cybersecurity" used worldwide; but, generally speaking, it refers to the preservation of the confidentiality, integrity and availability of digital information and its underlying infrastructure so as to ensure confidence in that information and infrastructure, and, ultimately, personal security both online and offline.

The means by which cybersecurity is achieved can include policy, technical and educational measures. For example, measures to protect confidential online information from being hacked include effective data protection laws and criminal laws against hacking (policy), the availability and use of strong encryption software (technology), and public awareness of how to create and use strong passwords (education).

A rights-respecting definition

A human rights-based definition of cybersecurity has been developed by Working Group 1 (Internet Free and Secure) of the Freedom Online Coalition:

"Cybersecurity is 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."

[Source]

Why is cybersecurity being discussed at the ITU?

The ITU's mandate to work on cybersecurity comes from the 2003 Geneva Plan of Action, one of the key outcome texts of the World Summit on the Information Society (WSIS), which tasked the ITU – and other organisations – with "Building confidence and security in the use of ICTs" (action line C5). Since then, ITU member states have given the ITU a more specific mandate to work on capacity-building on a range of cybersecurity-related issues, mostly through the ITU's Development Sector (ITU-D).

This mandate is limited; a fact acknowledged in Resolution 130, which was adopted at the ITU Plenipot in 2014:

"[The] ITU shall focus resources and programmes on those areas of cybersecurity within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights (...)"

Within that scope, the ITU's most significant mandated activities include:

- Maintaining a "cybersecurity gateway" as a means of sharing information on national, regional and international cybersecurity-related initiatives;
- Developing reports and recommendations which address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs (ITU-T);
- Supporting ongoing regional and global cybersecurity projects (ITU-D);
- Facilitating member states' access to resources developed by other relevant international organisations that work on national legislation to combat cybercrime (ITU-D);
- Supporting member states' national and regional efforts to build capacity to protect against cyberthreats and cybercrime (ITU-D);
- Assisting member states, in particular developing countries, in elaborating appropriate and workable legal measures relating to protection against cyberthreats at the national, regional and international levels (ITU-D);
- Establishing technical and procedural measures, aimed at securing national ICT infrastructures (ITU-D);
- Establishing organisational structures, such as Computer Incident Response Teams, to identify, manage and respond to cyberthreats, and cooperation mechanisms at the regional and international level (ITU-D); and
- Building the capacity of member states to protect against cyberthreats and cybercrime, as well to develop their national and/or regional cybersecurity strategies (ITU-D).

Why should human rights defenders care?

Strong cybersecurity can support the enjoyment and exercise of human rights, such as the rights to privacy and freedom of expression. However, measures put forward in the name of cybersecurity – often conflated with national security concerns – can sometimes have adverse effects on human rights; for example, attempts to restrict the availability of encryption at the national level, surveillance measures, intentional disruptions of online communication networks, and inappropriate criminal liability for online behaviour. Addressing internet policy issues primarily through a security lense has already led to limitations on open debate and the exclusion of critical voices.

As such, human rights defenders should be interested in cybersecurity generally. But there are three particular reasons to focus on cybersecurity discussions at the ITU.

- **Proposals for an international cybersecurity treaty:** Many voices have long been calling for an international cybersecurity treaty to be developed, and proposals at previous ITU conferences for this to happen under the auspices of the ITU. At the 2014 Plenipot, some member states proposed that the ITU "start reflection on the implementation of a global charter related to ICT security"; and, at the WTDC in 2017, there were proposals for the D-Sector's Secretary General to "start open multistakeholder consultations on the need of an international framework related to cybersecurity". While both proposals were ultimately rejected, the calls continue. From a human rights perspective, there are two particular concerns relating to any ITU-led treaty process. First, because, as noted above, at the national level, cybersecurity is often conflated with national security concerns with problematic laws and policies being developed. There is a risk that a treaty would reflect and exacerbate such national approaches with consequent threats to human rights. Second, because the ITU is a closed forum, any treaty negotiation process would likely exclude many stakeholders and critical voices, such as civil society organisations.
- **Cybersecurity-related standards**: Even if the ITU does not in the end develop a cybersecurity treaty, many states have pushed for its mandate on cybersecurity to expand from capacity-building to developing relevant standards. These could range from data protection laws to surveillance and data retention – issues with significant human rights implications, but where the ITU has little expertise. This would risk problematic national policies in certain countries feeding into international standards which are adopted elsewhere.
- **Capacity building**: As noted above, the ITU – particularly the D-Sector – does already have a mandate in relation to cybersecurity; from maintaining the "cybersecurity gateway" to sharing information and best practices on national, regional and international cybersecurity-related initiatives, and supporting member states in developing cybersecurity strategies. Here, the ITU plays a valuable role – its National Cybersecurity Guide, for example, has helped support rights-respecting cyber processes by sharing good practice. This existing work should be supported as a way of promoting similar good practices as more countries develop, and revise, their cybersecurity strategies.

Where is the discussion taking place?

Discussions around cybersecurity are taking place in a large number of forums within the ITU, including:

- In ITU-T Study Group 17 ("Security"), where question 4/17 looks at a range of cybersecurity issues;
- In ITU-D Study Group 2 ("ICT services and applications for the promotion of sustainable development") where question 3/2 focuses on best practices for developing a culture of cybersecurity;
- In the ITU-D Sector more broadly, where the activities listed above under "Why is cybersecurity being discussed at the ITU?" are coordinated and implemented.

It is likely that further discussions around cybersecurity will also take place at other upcoming ITU forums and events, including the Plenipotentiary Conference in October and November 2018.