10. Information and communication technology, cybersecurity and human development

Overview

This chapter considers the nexus between access to information and telecommunication technology (ICT), cybersecurity and human development.

For over a decade international organizations, including the United Nations Development Programme, the World Bank and the World Economic Forum, have repeatedly described (ICT) as a fundamental instrument of human development. ICT is expected to leverage socio-economic gains as it (a) provides an unprecedented ability for people to acquire capabilities (e.g. knowledge and skills); and (b) increases opportunities for people to use those capabilities for their own interest and for society as a whole. At it stands, there are no large-scale empirical studies that systematically and comprehensively assess the impact of ICT access for human development in developing countries. Some case studies have challenged the discourse of international organizations on the positive transformative power of ICT, illustrating that increased ICT access has not automatically led to effective life improvements of populations and has had, in some cases, disruptive effects as it has reinforced existing domination and inequalities between categories of the population, thereby generating tension or conflicts. Large-scale studies covering the impact of ICT for development have primarily attempted to consider the relationship between access to ICT and economic growth. These studies generally find a positive correlation between increased access to ICT and economic development (see section I).

Access to ICT may create new capabilities and opportunities for human development; at the same time it generates myriad risks that threaten people's ability to enjoy those opportunities (see section II). Cybercrime is of particular relevance to the extent that it directly undermines the ability of people and businesses to fully exploit the benefits of ICT and the Internet in particular. The insecurity that cybercrime generates ultimately has a palpable cost for national economies and economic development. There is therefore a growing understanding within the international development community that initiatives supporting greater access to ICT in the developing world need to integrate considerations for cybersecurity in order to be effective and sustainable. However, efforts to improve cybersecurity capabilities in developing countries may themselves create risks to human development, as security objectives of the state do not always coincide with the objectives and rights of individuals. Meth-

ods to fight cybercrime and pursue greater cybersecurity, such as increased cyber-surveillance and Internet filtering, may for instance have a detrimental effect on fundamental human rights and human security generally.

In the light of this, it is useful to conceptualize cybersecurity not only as a national security requirement but also as an essential component of human security. Approaching cybersecurity from a human security perspective requires a holistic approach that not only tackles risks related to cybercrime and sophisticated cyber-threats that jeopardize cyberspace, but also takes into account considerations of the principles of the rule of law and good governance that can improve people's trust in ICT. Notably, the process by which states may alter people's ability to enjoy the capabilities and opportunities generated by ICT based on national security considerations should be transparent, accountable and inclusive.

Developing countries are unequally equipped technically, politically and legally to deal with risks that access to ICT pose to human security. Increasingly, international and national development agencies see a need to couple initiatives democratizing access to ICT with efforts to strengthen national cybersecurity capabilities as well as digital human rights.

Initiatives supporting cybersecurity commonly entail policy and legal support (draft strategy, processes, guidance and laws), training and technical assistance (creation of dedicated agencies and computer emergency response teams) and cooperation. The International Telecommunication Union is currently the pivotal actor in terms of capacity building. Digital human rights and internet freedom are usually supported through direct assistance at the policy level (e.g. through definition of law on privacy and data protection, and the definition of standards for electronic surveillance). There are, however, no international standards for digital human rights, despite attempts by several organizations, such as the European Union and the Council of Europe, to define them. The definition of standards for electronic surveillance is also a contentious issue, inextricably intertwined as it is with the discussion on Internet governance. Recent efforts have therefore focused on directly and indirectly limiting the proliferation of electronic surveillance and censorship capabilities to countries that might use them to commit human rights abuses. In addition, a number of initiatives have or are being launched that directly empower people through education and capacity building in ICT security (see section III).

VINCENT BOULANIN