III. Mapping key actors and efforts in cybersecurity for human development

VINCENT BOULANIN

International and national development agencies increasingly see a need to couple initiatives democratizing access to information and communication technology (ICT) with efforts to strengthen national cybersecurity capabilities and digital human rights.[1] The following section identifies the key actors and efforts in cybersecurity for human development.

Cybersecurity capacity building

A number of initiatives have been undertaken in recent years to help developing countries improve their cybersecurity capabilities. Typically, these entail policy and legal support (draft strategy, processes, guidance and laws), training and technical assistance (creation of dedicated agencies and computer emergency response teams, CERT), and cooperation.

The International Telecommunication Union

The International Telecommunication Union (ITU) is currently a pivotal actor in terms of capacity building, mandated by the United Nations to support the development of cybersecurity capabilities globally. It played a leading role in the organization of the World Summit on the Information Society (WSIS), which covered a range of issues relating to ICT and development.[2] In 2007 the ITU launched its Global Cybersecurity Agenda (GCA) to provide a coordination framework for the international response to the growing challenge to cybersecurity.[3] The GCA was designed to enhance collaboration with and between all relevant partners to build confidence and avoid duplication of efforts. The GCA has five pillars: (*a*) legal measures, (*b*) technical and procedural measures, (*c*) organizational structures, (*d*) capacity building, and (*e*) international cooperation.

[1] Discussion of key actors working on increasing access to information and communication technology (ICT) and the Internet at the general level is beyond the scope of this section. Long-standing actors in this field include the International Telecommunication Union (ITU) and the World Bank. Newer initiatives include the Digital Development Partnership and the Alliance for Affordable Internet—a coalition of more than 60 actors from different sectors that aims to provide affordable and resilient Internet infrastructure in developing countries.

[2] The World Summit on the Information Society (WSIS) brought together international organizations, governments, business and civil society organizations. The first phase of the summit was held in Geneva in 2003, followed by a second phase held in Tunis in 2005.

[3] ITU, 'WSIS and building a global gulture of cybersecurity', [n.d.]; and ITU, Global Cybersecurity Agenda, <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>.

The ITU's capacity-building initiatives are primarily dedicated towards developing countries. The ITU published a guide to cybersecurity for developing countries in 2007.[4] In 2013 it launched a two-year project focusing specifically on least developed countries.[5] This project was intended to provide 49 countries with (*a*) policy-level assistance through customized guidelines on national cybersecurity legislation, regulations and technologies; (*b*) capacity building through workshops, training, events and training curricula; and (*c*) equipment and software.[6] In 2015 the ITU launched its Global Cybersecurity Index (GCI), which measures the level of engagement of countries in cybersecurity. The GCI is a useful tool for development agencies for identifying the actual needs of developing countries in terms of capacity building.

The European Union

Regional organizations are also increasingly engaged on the issue of cyber-related capacity building. The European Union (EU), for instance, has a variety of instruments that can directly or indirectly support the cybersecurity capabilities of third countries. One currently in use is the Instrument contributing to Stability and Peace (IcSP) that, among other things, supports the capability of law enforcement and judicial and civil authorities worldwide in the fight against organized crime, including cybercrime.[7] It serves notably to sponsor the Global Action on Cybercrime (GLACY), which promotes states' accession to the 2001 Council of Europe Convention on Cybercrime (Budapest Convention) and assists international cooperation between criminal justice authorities.[8]

The Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN) is also actively engaged in the issue of cybercrime. Adopted in 2002, the ASEAN Plan of Action to Combat Transnational Crime included training and capacity building as one main area of cooperation between its member states. This plan was followed

[4] ITU, *Cybersecurity Guide for Developing Countries, 2007* (ITU: Geneva, 2007).

[5] ITU, Enhancing Cybersecurity in Least Developed Countries project, <http://www.itu.int/en/ITU-D/Partners/Pages/Call4Partners/CYBLDC.aspx>.

[6] ITU, Enhancing Cybersecurity in Least Developed Countries, Concept Note, Sep. 2013.

[7] The Instrument contributing to Stability and Peace's (IcSP) budget for the period 2014–17 amounted to €2.3 billion, of which €10.5 million has been allocated to the fight against cybercrime and €11 million to cybersecurity. Deprez, N., 'Service for Foreign Policy Instruments (FPI): "The EU's Instrument contributing to Stability and Peace (IcSP)"', Presentation at Civil Society Dialogue Network Funding Instruments Meeting on the IcSP, Brussels, 17 Oct. 2014.

[8] Pawlak, P., 'Models for cybersecurity capacity building', ed. P. Pawlak, *Riding the Digital Wave: The Impact of Cyber Capability Building on Human Development*, European Union Institute for Security Studies (EUISS) Report no. 21 (EUISS: Paris, Dec. 2014), p. 67–70. Council of Europe, Cybercrime Programme Office, 'Global Action on Cybercrime: project summary', [n.d.]. Convention on Cybercrime of the Council of Europe (Budapest Convention), opened for signature 23 Nov. 2001, entered into force 1 July 2004.

in 2007 by the adoption of a common framework for ASEAN cybercrime enforcement capability building, and the creation of a working group on cybercrime in 2013.[9]

The Organization of American States

The Organization of American States supports the cyber-related capabilities of its member states via training, crisis management exercises and exchange of best practices through its Inter-American Committee against Terrorism (CICTE) and Cyber Security Programme.[10]

The African Union

The African Union (AU) does not conduct capacity building *per se*, but is actively working towards the harmonization of cyber-related legislation in African countries. In that regard, state members of the AU approved a Convention on Cyber Security and Personal Data Protection on 27 June 2014, which provides legal guidelines for cybercrime repression and protection of human rights online.[11]

Regional computer emergency response team networks

Regional CERT networks are also important actors in the development of cybersecurity capabilities as they may be both beneficiaries and facilitators of capacity-building initiatives. The Asia-Pacific CERT network, for instance, launched in 2014 the Green Project, which aims to establish a hub for collaboration efforts to address cybersecurity risks and improve the health of the cyber-ecosystem.[12]

Efforts to integrate digital rights considerations into cybersecurity

International and regional initiatives

Digital human rights and Internet freedom are typically defined and supported at the national policy level (e.g. through the definition of the law on privacy and data protection, and the definition of standards for electronic surveillance). There are, however, no international standards for digital human rights. Some organizations have made efforts to define them; the Council of Europe adopted a *Guide to Human Rights for Internet Users* in

[9] Association of Southeast Asian Nations (ASEAN), 'ASEAN's cooperation on cybersecurity and against cybercrime', Presentation by ASEAN Secretariat, at Octopus Conference on Cooperation Against Cybercrime, Strasbourg, 4 Dec. 2013.

[10] Organization of American States, Inter-American Committee against Terrorism, Cyber Security: Project description, <http://www.oas.org/en/sms/cicte/programs_cyber.asp>.

[11] African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV), opened for signature 27 June 2014, not yet in force.

[12] Pawlak (note 8), p. 69.

2014 and the EU published Guidelines on Freedom of Expression Online and Offline the same year.[13]

The definition of rights of individuals, groups and states online is, however, a contentious issue as it is inextricably intertwined with the discussion on Internet governance. This places countries such as China and Russia, which advocate stronger governmental control over the Internet, into opposition with liberal democracies, which favour multi-stakeholder models for Internet governance and the protection of Internet freedom.[14]

There are a number of forums where possible common standards for digital human rights are being discussed by international organizations, governments, civil society organizations and businesses. The 2015 Global Conference on Cyberspace, hosted by the Netherlands, for instance, had a notably strong focus on privacy protection.[15] The 10th annual meeting of the UN-mandated Internet Governance Forum, hosted by Brazil in 2015, also discussed the issues of cybersecurity and trust, as well as the Internet and human rights.[16] In that framework, the Freedom Online Coalition presented a number of comprehensive principles for cybersecurity and human rights.[17] In 2012 the Swedish International Development Cooperation Agency (SIDA), together with the Swedish Ministry for Foreign affairs and the Internet Foundation of Sweden, launched the Stockholm Internet Forum (SIF). The SIF is an annual international and multi-stakeholder event specifically dedicated to the promotion of human rights and development. The 2015 SIF focused on equal access to the Internet.[18]

Initiatives to improve human rights online are not only targeted at governments benefiting from development aid, they are also aimed at other key stakeholders. The UN, the Organisation for Economic Co-operation and Development (OECD) and certain governmental donors have called on private ICT companies to embrace responsible business practices and thereby support Internet freedom.[19] The UN guidelines on responsible business and human rights provide the basis for how ICT companies should proceed, and

[13] Council of Europe, Guide to Human Rights for Internet Users, Recommendation CM/Rec (2014)6, 16 Apr. 2014; and Council of the European Union, EU Human Rights Guidelines on Freedom of Expression Online and Offline, Foreign Affairs Council Meeting, Brussels, 12 May 2014.

[14] Klimburg, A. 'The Internet Yalta', Center for a New American Security Commentary, 5 Feb. 2013.

[15] Global Conference on Cyberspace, The Hague, 16–17 Apr. 2015. The previous conferences were held in London (2011), Budapest (2012) and Seoul (2013).

[16] Internet Governance Forum, João Pessoa, Brazil, 10–13 Nov. 2015.

[17] Freedom Online Coalition, 'Recommendations for human rights based approaches to cybersecurity', Working Group 1 discussion draft, 21 Sep. 2015.

[18] Stockholm Internet Forum, Stockholm, 21–22 Oct. 2015.

[19] Organisation for Economic Co-operation and Development (OECD), *Guidelines for Multinational Enterprises*, 2011 edn (OECD: 2011); United Nations, General Assembly, 'Guiding principles on business and human rights: implementing the United Nations "Protect, Respect and Remedy" Framework', Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, A/HRC/17/31, 21 Mar. 2011;

global standards for preventing and addressing the risk of adverse impact on human rights linked to business activity. Notably, it invites companies to conduct a process of human rights due diligence.

National initiatives

Governmental efforts to support digital rights are not limited to normative efforts on policy standards and best business practices. A number of states have taken direct action through their development aid programmes and export control regulations to support or preserve digital rights in developing countries.

Some states integrate information on online safety measures into their work with non-governmental organizations (NGOs), particularly human rights organizations, in developing countries. Sweden, for example, includes such measures, which can cover education on ICT security and circumventing censorship and filtering, in almost all the pro-democracy and human rights programmes managed by its development agency—SIDA.[20] SIDA has also previously supported the development and distribution of technologies (such as operating systems) that allow anonymous Internet activity.

Allegations of human rights abuses related to the use of western cyber-surveillance technologies by authoritarian regimes have also led states to update their export control regulations to prevent the proliferation of surveillance technologies to countries that might use them to commit human rights abuses. These changes have been coordinated within the framework of the Wassenaar Arrangement.[21] Since 2010, the 41 member states of the Wassenaar Arrangement have successively agreed on the introduction of controls on mobile telecommunication jamming equipment (2010), interception and passive countersurveillance equipment (2012), and malware-based surveillance products and Internet Protocol (IP) network monitoring systems (2013).[22]

Private sector initiatives

The ICT sector has also set up its own initiatives on Internet freedom and privacy, including the Global Network Initiative at the Silicon Valley Human Rights Conference and the Telecommunications Industry Dialogue. These

and Swedish Ministry for Foreign Affairs (MFA), Enhancing Internet Freedom and Human Rights Through Responsible Business Practices (MFA: Stockholm, 2012).

[20] Swedish International Development Cooperation Agency (SIDA), 'Freedom of expression', 2 Dec. 2009.

[21] Wassenaar Arrangement, <http://www.wassenaar.org/>.

[22] For further discussion of the introduction of new controls on surveillance technologies see Bromley, M. et al. 'ICT surveillance systems: trade policy and the application of human security concerns', *Strategic Trade Review*, vol. 2, no. 2 (2016); and SIPRI/Ecorys, *Final Report: Data and Information Collection for EU Dual-use Export Control Policy Review* (European Commission: Brussels, Nov. 2015), p. 142.

initiatives are working towards the creation of guiding principles for corporate social responsibility in the ICT sector.[23]

A number of NGOs are also very active in supporting ICT companies in the development of corporate responsibility practices. The Institute for Human Rights and Business in the United Kingdom, for instance, aids telecommunications companies to evaluate their impact in terms of human rights.[24] In 2015 the NGO-based initiative 'Ranking Digital Rights' rated the transparency of telecommunications and Internet companies in relation to human rights, with a clear focus on end-user privacy.[25] In addition, the UN Special Rapporteur for Freedom of Expression, David Kaye, launched an initiative in 2016 to identify possible guiding principles for corporate responsibility in the telecommunications sector.[26] Some companies have also devised internal practices to understand and manage their impact on human rights: for example, Swedish telecommunications company Ericsson holds what it terms 'human rights impact assessments' before entering sensitive markets.[27]

Civil society initiatives

As noted above, NGOs play a critical role in the defence of digital rights. NGOs such as Amnesty International, the Electronic Frontier Foundation, Human Rights Watch and Privacy International are working in various forums to obtain clear definitions of the standards for digital human rights. Some are also developing capacity-building initiatives intended to empower individuals and grass-roots organizations through ICT security.

Conclusions

A number of stakeholders are working towards improving cybersecurity capabilities and digital rights in developing countries. These initiatives remain poorly coordinated, however, and in some cases they are pursuing conflicting objectives: initiatives aimed at improving a state's cybersecurity capabilities might also negatively impact on the digital rights of the citizens of that state. Alternatively, efforts to improve the right to privacy and freedom of expression of individuals in the digital realm might put in place hurdles to a state's ability to provide cybersecurity as a public good. Thus,

[23] Global Network Initiative (GNI), *2014 Annual Report* (GNI: Washington, DC, 2014); and Telecommunications Industry Dialogue (TID), *Telecommunication Industry Dialogue at Two Years: Advances in Respecting Freedom and Privacy in 2014* (TID: Washington, DC, May 2015).

[24] Institute for Human Rights and Business, 'Digital dangers: identifying and mitigating threats to human rights in the digital realm', [n.d.].

[25] Ranking Digital Rights, Ranking Digital Rights Corporate Accountability Index, 2015.

[26] Office of the United Nations High Commissioner for Human Rights (OHCHR), 'Call for submissions: freedom of expression and the private sector in the digital age', [n.d.].

[27] Ericsson, *ICT and Human Rights: An Ecosystem Approach*, (Ericsson: Stockholm, 2013).

the international development community has more work to do before it can implement a comprehensive and integrated approach to cybersecurity capacity building that adequately balances national security and human security considerations. To meet this challenge, some studies have suggested that the international development community could draw useful lessons from past and current initiatives in the area of security sector reform, where the challenges are of a similar nature.[28]

[28] Muller, L. P., 'Cyber security capacity building in developing countries', Norwegian Institute of International Affairs (NUPI) Policy Brief no. 15 (2015); Tagert, A. C., *Cybersecurity Challenges in Developing Nations*, Dissertation Paper 22 (Carnegie Mellon University: Pittsburgh, PA, Dec. 2010); and Pawlak (note 8), p. 16.