II. Cybersecurity: a precondition to sustainable information and communication technology-enabled human development

VINCENT BOULANIN

Access to information and communication technology (ICT) creates new capabilities and opportunities for human development; at the same time, ICT also constitutes a powerful new medium for various kinds of illicit, anti-social and threatening activities that can put human development at risk.[1] There is a growing understanding that initiatives supporting greater access to ICT in the developing world (often grouped under the term 'ICT for development', ICT4D) need to integrate cybersecurity considerations in order to be effective and sustainable.[2]

New risks to human development

Access to ICT generates myriad risks that threaten people's trust in ICT and their well-being in cyberspace. Two of them, cybercrime and cyber-surveillance, are of particular relevance to the extent that they directly threaten two important aspects of human security that were highlighted by the United Nations Development Programme's (UNDP) *Human Development Report 1994*—namely, freedom from want and freedom from fear.[3]

[1] Risks associated with the use of information and communication technology (ICT) are usually classified in the cybersecurity literature in 2 categories: risks *to* cyberspace and risks through cyberspace. 'Cyberspace' is here defined as a bioelectronics environment that is characterized by the connection and interdependence between ICT and information thereon. Risks to cyberspace are those of a technical nature. They include 'attacks' on ICT but also vulnerability 'failure' and 'accident', which may undermine the availability, confidentiality or integrity of ICT and information resident thereon. Risks through cyberspace refer to the challenges produced by cyberspace as a new medium from anti-social, illicit or threatening activities, ranging from harassment, vandalism, fraud, organized crime, terrorism and espionage to warfare. Deibert, R. J. and Rohozinski, R., 'Risking security: policies and paradoxes of cyberspace security', International Political Sociology, vol. 4, no. 1 (2010), pp. 15–32.

[2] In contrast to common definitions of 'cybersecurity' that focus on the technical—securing the availability, confidentiality and integrity of ICT and information thereon—or are directly relevant to national security (such as the state or critical infrastructures), cybersecurity is approached here from a human security perspective. Cybersecurity is about ensuring people's ability to enjoy the capabilities and opportunities offered by ICT, and thereby their well-being in cyberspace, by preventing and reducing the risks stemming from access and use of ICT. In accordance with concepts proposed by Pawlak, this analysis not only includes risks posed by states and non-state actors to other states and their citizens, but also includes risks resulting from a state's negligence or premeditated actions against its own citizens, e.g. abusive surveillance. Pawlak, P., 'Introduction', 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).

[3] Porcedda, M. G., 'Rule of law and human rights in cyberspace', ed. Pawlak (note 2), p. 33.

Cybercrime

According to the International Telecommunication Union (ITU), 'cybercrime' refers to a large variety of illegal activities committed by means of, or in relation to, a computer system or network.[4] These illegal activities include the following:

1. *Offences against the availability, integrity and confidentiality of ICT and information thereon*. This category covers technical offences such as illegal access, illegal data acquisition, illegal interception and data interference.
2. *Content-related offences*. This category concerns the diffusion or use of illegal content, including child pornography, spam and xenophobic or hateful material or material glorifying violence.
3. *Copyright- and trademark-related offences*. This category concerns the violation of copyright- and trademark-protected material of any kind, such as music, video and text, for instance, via file-sharing systems or peer-to-peer network services.
4. *Computer-related offences*. This category covers non-ICT specific offences that may be performed via the use of a computer. These include computer-related fraud or forgery, phishing, identity theft and cyber-laundering.
5. *Terrorist use of the Internet*. This category criminalizes the use of ICT for terrorist purposes, including propaganda, information gathering, publication of training material, terrorist financing and attacks against critical infrastructure.

These activities threaten human development as they fundamentally undermine people's trust in ICT as well as their well-being in cyberspace. Offences against the availability, confidentiality and integrity of ICT may discourage people and businesses from engaging in greater use of ICT. Content-related offences contribute to making cyberspace a hostile environment and may discourage some proportion of the population, notably minority groups, from fully exploiting the benefits of ICT and the Internet in particular. Copyright- and trademark-related offences may dissuade people, businesses and institutions from digitalizing and making available online cultural or educational content. Computer-related offences are also often the cause behind major economic loss for people, businesses and governmental institutions.

There is a direct correlation between ICT connectivity—that is, access to the Internet—and cybercrime. The higher a country's level of Internet connectivity, the higher the likelihood that people in that country will be affected by cybercrime. Reports suggest that once a developing country has

[4] International Telecommunication Union (ITU), *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (ITU: Geneva, Sep. 2012), pp. 12–73.

introduced broadband connectivity, there tends to be a steep and immediate rise in cybercrime in that country.[5] As the number of Internet users in the world has grown, cybercrime has increased exponentially. The cybersecurity company Symantec reported that the total number of security breaches worldwide in 2013 was 62 per cent greater than in the previous year.[6] Most of the reported incidents in 2013 were phishing and identity theft for financial fraud through social media sites. The cybercriminals carrying out these offences primarily targeted individual users.[7] They are now increasingly targeting mobile Internet connection platforms, which are the main source for connectivity for people living in developing countries.

The insecurity that cybercrime generates ultimately has a palpable cost for national economies. In a report by McAfee and the Centre for Strategic and International Studies (CSIS), the annual cost of cybercrime to the global economy was estimated to be more than $400 billion—representing a global average loss of 0.5 per cent of gross domestic product (GDP).[8] In addition, Europol estimated that Internet crime was now more profitable than the global trade in cocaine, heroin and marijuana combined.[9]

Most of the economic losses attributable to cybercrime were recorded in developed countries. Quantifying the impact of cybercrime in developing countries remains difficult due to a lack of data. The McAfee and CSIS report on the global cost of cybercrime did not include, for instance, data on the large majority of countries situated in Africa, South East Asia or Central and Latin America.[10] However, the report did identify a clear correlation between cybercrime and national income level. Wealthier countries have higher levels of Internet connectivity, and hence the people, businesses and institutions in those countries are more likely to be affected by cybercrime.[11] Middle-income countries were therefore more affected by cybercrime than least developed countries. In 2015 the losses suffered by Brazil, China and India as a result of cybercrime represented 0.32, 0.63 and 0.21 per cent of their respective GDPs. In contrast, losses caused by cybercrime in Nigeria

[5] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II* (McAfee: Santa Clara, CA, June 2014), p. 6.

[6] Symantec Corporation, *Internet Security Threat Report 2014*, vol. 19 (Symantec Corporation: Mountain View, CA, Apr. 2014), p. 5.

[7] Symantec Corporation, *Internet Security Threat Report 2013*, vol. 18 (Symantec Corporation: Mountain View, CA, Apr. 2013); and Center for Strategic and International Studies (note 5).

[8] Center for Strategic and International Studies (note 5). Developing countries record less net loss than developed countries. However, the effect of cybercrime is nonetheless significant, notably for employment. Robinson, N., 'Building blocks for strengthening cybersecurity capacities', ed. Pawlak (note 2), p. 18.

[9] Pawlak, P., 'Developing capabilities in cyberspace', ed. Pawlak (note 2), p. 9.

[10] The absence of data on cybercrime is certainly correlated to the comparatively low level of penetration of ICT, and broadband Internet in particular, in these countries.

[11] Because it takes the same amount of effort to hack a valuable target as a not so valuable target, cybercriminals 'gravitate to the places where value online is the highest'. Center for Strategic and International Studies (note 5), p. 8.

and Kenya in 2015 represented only 0.14 and 0.01 per cent of their respective GDPs. While developing countries have comparatively less to lose, this does not mean that the threat of cybercrime is not problematic.[12] Cybercrime may have the potential to jeopardize the socio-economic gains that developing countries enjoy thanks to growing access to ICT. Like developed countries, developing countries therefore need to put significant effort into enhancing their cybersecurity and cyber-resilience capabilities.

Cyber-surveillance

Efforts to improve cybersecurity capabilities in developing countries may themselves create risks to human development. The security objectives of the state do not always coincide with those of individuals. Also, the methods used to pursue greater cybersecurity at the national level may have a detrimental effect on fundamental human rights.

For governments, fighting cybercrime and defending against cyberthreats originating from states and non-state actors require not only passive protection capabilities (e.g. firewalls and anti-virus measures) but also surveillance and network monitoring capabilities that will enable them to observe and record online behaviours, as well as conduct investigations to ascertain the identities of people and platforms on ICT networks.[13] The typical rationale used by governments to justify these activities is that ICT and the Internet have provided criminals, terrorists and states harbouring wrongful intentions with the ability to communicate anonymously and conduct malicious operations in ways that did not previously exist. Notably, they use encryption and other techniques to conceal their activity and stay out of reach of law enforcement authorities and the intelligence community.[14]

Law enforcement, intelligence and military professionals are therefore increasing their demand for solutions and techniques that will enable them to break or bypass encryption, such as compelling ICT providers to have a back-door in their system allowing access to users' private data.[15] Additional methods include compromising ICT devices with intrusion software.[16] In the wrong hands these capabilities may be abused by governments and lead to violations of human rights, including not only those directly applicable

[12] On the benefits and costs of cyber-activities using ICT see Hathaway, M., 'Cyber readiness index 1.0', slide 11, presentation at Belfer Center for Science and International Affairs, Harvard Kennedy School, Harvard University, Cambridge, MA, 7 Nov. 2013.

[13] TechUK, *Assessing Cyber Security Export Risks* (TechUK: London, Nov. 2014).

[14] Anderson, D., *A Question of Trust: Report of the Investigatory Powers Review* (The Stationery Office: Norwich, June 2015).

[15] A famous example is the United States' National Security Agency's (NSA) PRISM surveillance programme, the existence of which was revealed by whistleblower Edward Snowden. Greenwald, G., 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June 2013.

[16] Insider Surveillance, The Little Black Book of Electronic Surveillance: 2015, 2nd edn (Insider Surveillance: Feb. 2015); and Privacy International, 'Communications surveillance', [n.d.].

to ICT use (such as right to privacy, freedom of expression and freedom of association), but also rights that directly relate to bodily integrity (such as the right to life, freedom from arbitrary arrest and detention, and freedom from torture and inhumane or degrading treatment).[17] In this regard, the events of the 2011 Arab Spring revealed the large spectrum of physical human rights abuses that could be related to electronic surveillance. Allegedly, governments in Egypt, Libya, Syria and Tunisia made extensive use of electronic surveillance capabilities to find and monitor political opponents who, in some cases, later became victims of arbitrary arrests and cases of torture and degrading treatment.[18] Privacy advocates, including the organization Privacy International, are therefore critical of the proliferation of surveillance technologies. They denounce the lack of control on the trade of these technologies, as well as the absence of international standards of lawful surveillance.[19]

To combat content-related offences, governments across the globe are tending to use censorship at various levels. There are a number of techniques that can be used to filter and block Internet content. Typically, governments can either filter and block content at the source by filtering traffic at key intersections of the network, or request Internet content providers to take down content that is judged illegal or inappropriate, ranging from single web pages, blogs, videos and articles to entire websites. Major companies such as Facebook, Google and Twitter now publically disclose the number of requests they receive annually as well as their compliance rate. The figures reported by Twitter show that such requests have increased dramatically in recent years. In the three years it has released data, the number of requests received by Twitter has risen from 6 to 1003.[20]

A major problem with censorship is that states have different understandings of the types of content that can be classified as illegal, leading to tension between these states and Internet content providers. Facebook, Google and Twitter have reportedly been blocked in China because they refused to comply with some governmental requests.[21] Such radical measures have

[17] McKune, S., 'Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries', Hearing of the European Parliament, Brussels, 21 Jan. 2015.

[18] Wagner, B., *After the Arab Spring New Paths for Human Rights and the Internet in European Foreign Policy*, European Parliament, Directorate-General for External Policies, Briefing Paper, EXPO/B/DROI/2011/28 (European Parliament, Directorate-General for External Policies: Brussels, July 2012).

[19] Anderson, C., 'Export controls in the digital age: the EU export control policy review and surveillance technology', WorldECR, no. 38 (Mar. 2015); Omanovic, E., 'Considerations on Wassenaar Arrangement control list additions for surveillance technologies', accessnow.org, 13 Mar. 2015); and Coroama, V. et al., 'Emerging smart surveillance technologies', eds M. Friedenwald and R. Bellanova, Smart Surveillance: State of the Art (Fraunhofer Institute for Systems and Innovation Research ISI: Karlsruhe, 2012).

[20] Freedom House, *Freedom on the Net 2015* (Freedom House: Washington, DC, Oct. 2015), p. 7.

[21] Freedom House (note 20), p. 7.

prompted a growing number of companies to proactively police content on their platforms. Some countries allegedly also use more coercive methods to have content removed, including direct pressure on individuals through intimidation, interrogation and arrest.[22]

If electronic surveillance could be said to potentially threaten one essential component of human security, namely freedom from fear, then censorship brings with it the risk of depriving people of another component of human security, namely freedom from want.[23] Censorship limits people's ability to enjoy free and open access to the Internet and thereby their capacity to access and use information they value.

Cybersecurity for human development

Approaching cybersecurity from a human security perspective

It is useful to conceptualize cybersecurity not only as a national security requirement but also as an essential component of human security.[24] Behind all information and communication infrastructures and devices there are human beings whose well-being and rights need to be protected.[25] 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 for principles of the rule of law that can improve people's trust in ICT.[26] This approach includes taking legal action to (*a*) clarify what law regulates the conduct of public and private actors in cyberspace; (*b*) prohibit arbitrariness of executive powers by introducing safeguards and strict permissible limitations; (*c*) ensure conviction of cybercriminals; (*d*) ensure non-discrimination and equality before the law; and (*e*) guarantee respect of human rights.

Cybersecurity capabilities in the developing world

Until 2015 assessing cybersecurity capabilities of developing countries remained difficult. Past attempts to evaluate countries' cybersecurity readiness had limitations in terms of methodology or scope. The United Nations Institute for Disarmament Research's (UNIDIR) Cyber Index, published in 2013, mapped countries individually and did not provide models for

[22] Freedom House (note 20), p. 8.

[23] Porcedda (note 3), pp. 29–41.

[24] Dunn Cavelty, M., 'Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities', *Journal of Science and Engineering Ethics*, vol. 20, no. 3 (Sep. 2014), pp. 701–15.

[25] 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.

[26] For a more detailed discussion see Porcedda (note 3).

Table 10.3. Cybersecurity capabilities by region and type of measures according to the Global Cybersecurity Index, 2014

Ranking is from 0 (lowest) to 1 (highest).

Area	Legal	Technology	Organizational	Capacity building	Cooperation	Overall index
Africa	0.31	0.13	0.17	0.11	0.16	0.16
Americas	0.44	0.24	0.24	0.25	0.20	0.26
Arab States	0.42	0.24	0.27	0.26	0.23	0.27
Asia–Pacific	0.41	0.30	0.30	0.27	0.25	0.29
CIS	0.73	0.31	0.19	0.13	0.26	0.27
Europe	0.79	0.42	0.45	0.37	0.34	0.45
World	0.50	0.27	0.28	0.24	0.34	0.28

CIS = Commonwealth of Independent States.

Source: International Telecommunication Union (ITU)/ABI Research, Global Cybersecurity Index, 2014, p. 17.

comparison.[27] Moreover, it was never updated. The Cyber Readiness Index produced by the Belfer Center at Harvard University chose a more systemic comparative approach but focused on only 35 countries, which were, in the majority, developed economies.[28]

In 2015 the ITU launched its Global Cybersecurity Index, which is geographically the most comprehensive coverage to date. The Index measures the commitment of countries to cybersecurity.[29] It assesses the level of development in five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation. At a regional level, the figures for 2014 showed that commitment to cybersecurity was lowest in Africa and highest in Europe.[30] The Index found that, globally, national cybersecurity efforts have so far focused primarily on legal aspects (see table 10.3).

A study by Microsoft, published in 2014 and entitled *Linking Cybersecurity Policy and Performance*, provides a useful complement to the ITU's Global Cybersecurity Index as it assesses not only the level of states' engagement in cybersecurity, but also the level of risk for Internet users in these countries. The study compared the cybersecurity performance of more than 100 countries based on a model combining data on the number of computers infected with viruses or malware in each country, socio-economic factors, and policy

[27] United Nations Institute for Disarmament Research (UNIDIR), *The Cyber Index: International Security Trends and Realities* (UNIDIR: Geneva, 2013).

[28] Hathaway (note 12).

[29] ITU and ABI Research, *Global Cybersecurity Index and Cyberwellness Profiles Report 2014* (ITU/ABI Research: Geneva, Apr. 2015).

[30] ITU and ABI Research (note 29).

choices related to cybersecurity.[31] It regrouped countries based on their performance—effective, moderate and low—and found that, in the large majority of cases, the countries with the lowest level of cybersecurity were from developing regions: 52 per cent were located in Africa and the Middle East, 21 per cent in Asia Pacific, 17 per cent in Latin America and the Caribbean, and the remaining 10 per cent were located in Central and Eastern Europe.

Other sources of statistics on malware infection also corroborate that developing countries generally remain unsafe environments for ICT use. A top 20 ranking covering 2014, compiled by Russian cybersecurity company Kaspersky Lab, heavily featured developing countries as states where users face the greatest risk of online infection.[32] This was equally true for the ranking on the highest level of local infection.[33]

Human security in cyberspace: completing the picture

The aforementioned studies have a strong technical and hard security focus and do not give a complete picture of the extent to which developing countries provide a safe and secure digital environment for their citizens. Notably, they do not give any indication of the degree of freedom and privacy those citizens may enjoy in cyberspace. Thus, reports on digital human rights and Internet freedom provide a useful complement.

According to Freedom House's Internet Freedom Index 2014–15, published in its annual *Freedom on the Net* report, Internet freedom around the globe declined in 2014–15.[34] The study covered development in 65 countries between June 2014 and May 2015. Based on a comparison with previous years, the report concluded that in 2014–15: (a) a larger number of governments censored public information of public interest than had previously

[31] The report did not report on capabilities of individual countries; instead it identified 3 clusters: 'maximizers', 'aspirants' and 'seekers'. Maximizers are countries with effective cybersecurity capabilities; aspirants are countries with a moderate level of cybersecurity; and seekers are countries with a low level of cybersecurity. Kleiner, A., Nicholas, P. and Sullivan, K., *Linking Cybersecurity Policy and Performance*, (Microsoft Trustworthy Computing: Redmond, WA, 2014).

[32] In order to assess the countries in which users most often face cyber-threats, Kaspersky Lab calculated how often its users encountered detection verdicts on their computers in each country. The resulting data characterizes the risk of infection that computers are exposed to in different countries across the globe, providing an indicator of the level of risk of cyber-threats facing computer users in different parts of the world. In 2014 the top 20 in order were (1) Russia, (2) Kazakhstan, (3) Azerbaijan, (4) Viet Nam, (5) Armenia, (6) Ukraine, (7) Mongolia, (8) Belarus, (9) Moldova, (10) Kyrgyzstan, (11) Germany, (12) Algeria, (13) Qatar, (14) Tajikistan, (15) Georgia, (16) Saudi Arabia, (17) Austria, (18) Lithuania, (19) Sri Lanka, (20) Turkey. Kaspersky Lab, 'Kaspersky security bulletin 2014', 1 Dec. 2014, pp. 32–33.

[33] 'Local infection' refers to a threat that has penetrated the operating system of a computer through something other than the Internet, email or network port. In 2014 the top 20 countries where users faced the highest risk of local infection were, in order (1) Viet Nam, (2) Mongolia, (3) Nepal, (4) Bangladesh, (5) Yemen, (6) Algeria, (7) Iraq, (8) Laos, (9) India, (10) Cambodia, (11) Afghanistan, (12) Egypt, (13) Saudi Arabia, (14) Kazakhstan, (15) Pakistan, (16) Syria, (17) Sudan, (18) Sri Lanka, (19) Myanmar, (20) Turkey. Kaspersky Lab (note 32), pp. 36–37.

[34] Freedom House (note 20).

done so; (b) overall, the number of individuals jailed by state authorities for supposedly unlawful acts of online expression was significantly higher than in previous years; and (c) the overall level of state cyber-surveillance power increased as bans on encryption and anonymity tools became more commonplace.

The large majority of the 32 countries that followed a negative trajectory (i.e. reduced the level of freedom online) in 2014–15 were developing countries; some wealthier countries were included among the 32, but these were countries with a poor general record in democratic development (e.g. Saudi Arabia). Two of the countries that showed the sharpest decline in the Internet Freedom Index were affected by internal conflicts in 2014–15: Libya and Ukraine. The five 'least free' countries in the world were, in order, China, Syria, Iran, Ethiopia and Cuba. Out of 15 Asian countries covered by the study, 8 were ranked as 'partly free' and 5 were listed as 'not free', with China, Myanmar, Pakistan, Thailand and Viet Nam receiving the poorest scores. Japan and the Philippines were the only countries in Asia considered to be 'free'. In sub-Saharan Africa, Kenya and South Africa were the only 'free' countries out of the 12 covered by the study. The majority (seven countries) were considered to be 'partly free' and three—Gambia, Ethiopia and Sudan—were listed as 'not free'. In Latin America, the majority of the countries listed were ranked as 'partly free'; Cuba had the poorest score, while Argentina and Brazil were listed as 'free' countries. The study found no 'free' country in the Middle East and North Africa. Five were listed as 'partly free' and another six were listed as 'not free': Bahrain, Egypt, Iran, Saudi Arabia, Syria and the United Arab Emirates.[35]

The study also estimated that of the 3 billion people with access to the Internet in 2014–15, (*a*) 61 per cent lived in countries that censored online criticism of the government, the military or the ruling family; (*b*) 47 per cent resided in countries where people had been attacked or killed for their online activity since June 2014; (*c*) 47 per cent lived in countries where corruption allegations against top government figures could be repressed or punished; (*d*) 45 per cent resided in countries where posting of satirical content online could result in censorship or jail time; (*e*) 34 per cent lived in countries where LGBT (lesbian, gay bisexual and transgender) voices were censored; (*f*) 38 per cent resided in countries where major social media and online messaging applications were blocked; and (*g*) 34 per cent lived under a government that had disconnected Internet and mobile phone access in 2014–15.[36]

Although Freedom House's report shows a clear diminution of Internet freedom globally, it also notes that access to ICT continued to positively

[35] Freedom House (note 20), pp. 16–17.
[36] Freedom House (note 20), p. 15.

support the activities of activists, civil society organizations and journalists that defend human rights and democratic reforms. One piece of anecdotal evidence was the release of five of the nine bloggers who were tried in Ethiopia for terrorism charges, following an Internet campaign demanding their release which gained global attention with the hashtag #FreeZone9Bloggers.[37] Some countries also improved their track record remarkably over the course of 2014–15. Notably, Sri Lanka lifted censorship on a number of previously inaccessible websites, while Zambia reduced major restrictions on online content.[38]

[37] Freedom House (note 20), p. 2.
[38] Freedom House (note 20), p. 3.