BRIEFING DOCUMENT: CYBERSECURITY POLICY AND HUMAN RIGHTS

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

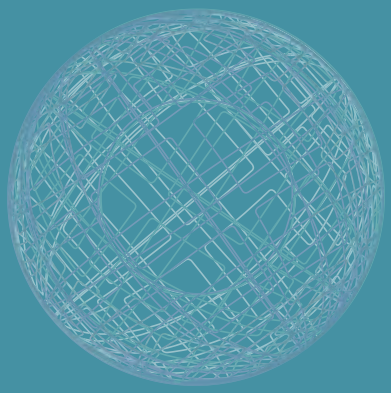
Briefing document:
Cybersecurity policy
and human rights

Written by:
Deborah Brown
Anriette Esterhuysen
Mallory Knodel

Editor:
Lori Nordstrom

Layout design:
Cathy Chen

ISBN 978-92-95102-95-8
APC-201712-GAPS-R-EN-DIGITAL-285



About this document

This briefing document aims to frame discussions at the Internet Governance Forum (IGF) 2017 Day 0 event “A rights-based approach to cybersecurity: A pipe dream or a critical means to a secure and stable internet?”. The goal of this event, and therefore this briefing document, is to deepen understanding of the human rights dimensions of cybersecurity policy in 2017. It touches on major developments in the field of cybersecurity that impact on human rights, and maps out key issues for further discussion at the Day 0 event. This briefing is not meant to be comprehensive. For example, by focusing on policy and normative approaches to cybersecurity threats, it does not address in detail the important responses from the technical and academic communities in this regard. Discussion, debate and additional contributions are welcome.

Introduction

Statements that efforts to establish a secure and stable internet must respect and promote human rights have almost become a mantra in multistakeholder internet governance spaces, like the IGF. In reality, however, most cybersecurity policy development efforts tend to do little more than pay lip service to human rights. Many contain provisions that threaten or undermine rights.

It also seems that the general public alarm following the Snowden revelations has settled down, and the internet has become this platform that no one really trusts, but that everyone uses anyway, because they are so dependent on it. Widespread cybersecurity incidents, like WannaCry, a ransomware attack that infected computers in over 150 countries within a day, disrupting some hospitals, banks, and telecommunications companies[1] and resulting in up to USD 4 billion in economic loss,[2] may have increased awareness and wariness around the insecurity of internet-connected devices. A further factor that is shifting the context of this mistrust is the fact that in a number of countries where the state – including some authoritarian states – has lacked capacity in the field of cybersecurity, it has outsourced its responsibilities in this area, as well as monitoring and intercepting user communications and online activity, to private sector service providers. This not only decreases transparency; it also makes lack of clear accountability even murkier. However, the wider impact of this mistrust is not yet clear and therein lies the danger, particularly with regard to the slow, global chilling effect it is likely to have on democratisation and freedom of expression and association.

It is the intention of the organisers of this event to delve deeper and enable the articulation of a shared vision for a secure and stable internet that is rights-based, both at the level of policy, norms and standards and at the level of technical architecture and protocols. That vision can be strengthened by research, analysis and network building to facilitate joint and coordinated efforts by different stakeholders in a variety of forums.

What follows is an initial overview of current trends and ideas for such future work and collaboration. It begins by defining cybersecurity and its sub-elements. Using that framework, it identifies some of the major cybersecurity incidents in 2017 followed by a listing and brief analysis of some key cybersecurity policy processes and trends.

Defining cybersecurity

Cybersecurity can signal a wide range of concerns and areas of work. As we view cybersecurity as something that complements a human rights and international humanitarian law framework, we use "cybersecurity" as defined by the Freedom Online Coalition (FOC) in 2015, which is prefaced with the text: "International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights."

The FOC definition of cybersecurity is as follows:

> 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.[3]

It continues to define the terms "availability", "confidentiality" and "integrity" in more detail, drawing on the ISO 27000 standard:

> Availability is a property of being accessible and usable upon demand by an authorised entity.

1. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know
2. https://cybercrime.truecrimelover.com/2017/09/25/total-wannacry-losses-pegged-at-4-billion
3. https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog8

Confidentiality is a property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Integrity is a property of accuracy and completeness.

Cybersecurity threats and incidents in 2017

Incidents that generate forms of cyber "insecurity" and threats are increasing. They range from actions taken by governments such as internet shutdowns, censorship and filtering to large-scale breaches in data security. According to a report by Accenture cited in TechRepublic, the five most common threats in the first half of 2017 were reverse deception tactics; sophisticated phishing campaigns; strategic use of information operations (cyberattacks and cyberespionage used by nation-states and other actors); alternative crypto-currencies; and DDoS-for-hire services.[4]

The security of cyberspace, according to the FOC definition above, means that information and the infrastructure that is needed to share it is (1) available, (2) confidential and (3) retains its integrity. Below is a glance at some of the major cybersecurity failures in 2017, categorised according to these three qualities. Viewing these incidents sets us up to look at the parallel responses from each sector by region in the next section.

Availability

In today's digital age, the availability of internet connectivity and information obtained online is critical in multiple ways. As more and more basic day-to-day functions and transactions rely on connectivity, internet shutdowns, either accidental or intentional, are major disruptions not just to the internet network itself but to people's daily lives. It is in this context that the intentional disruption or prevention of access to or dissemination of information online is a violation of international human rights law, according to the UN Human Rights Council.[5]

Often, network disruptions occur when connectivity between people is most important, whether as a result of natural disasters or a response to political crisis. There were several incidents of intentional internet shutdowns in 2017, some of which are cited below. The majority of these occurred in the global South, disproportionately affecting already fragile communities by impacting the economy, communications and information dissemination. Just a few examples include:

- Cameroon: 93 days, full network shutdown in the Anglophone region of the country due to protest over marginalisation by the Francophone-led government.[6]
- India: Over the course of three months, various incidents in Kashmir Valley, Nagaland and West Bengal, such as political unrest and election violence, led to sites being blocked, network slowdowns and service blockage.
- Syria: A full network shutdown nationwide for 15 days was reported by a confidential source to Access Now.[7]
- Togo: The Togolese government first shut down mobile internet services in the country for six days in September in response to a wave of protests against the ruling government. This shutdown was met with wide condemnation from internet freedom groups across the globe and the government grudgingly restored services after six days of blackout.[8] However, the government continued to shut down or restrict access repeatedly during the following few months. Local protests continued but the international outcry did not. This is a common trend in responses to shutdowns.[9]

4. https://www.techrepublic.com/article/report-the-top-5-cybersecurity-threats-of-2017
5. https://undocs.org/en/A/HRC/RES/32/13
6. http://www.cnn.com/2017/02/03/africa/internet-shutdown-cameroon/index.html
7. https://www.accessnow.org/keepiton-shutdown-tracker
8. www.africanews.com/2017/09/11/internet-restored-in-togo-after-6-days-opposition-mulls-next-move/
9. https://www.apc.org/en/pubs/civil-society-organisations-write-international-bodies-over-internet-shutdown-togo

Distributed denial of service (DDoS) attacks are a popular method to make online content or platforms unavailable. While DDoS attacks are usually only for a finite period of time, they can have lasting damage to the platform or website itself as it tries to recover reputation, affordable hosting contracts, and business lost during the outage. Three reports on major DDoS incidents against civil society organisations were published this year by APC member eQualit.ie, which provides DDoS mitigation services through its software Deflect. These attacks were launched against the Kotsubynske independent media news site in Ukraine,[10] Black Lives Matter in the United States,[11] and groups supporting the Boycott, Divestment and Sanctions movement.[12]

Availability is also tied to the issue of integrity when it comes to malware that has the intention to limit or shut down the availability of a website. That is covered in the sub-section below on integrity.

Confidentiality

When an increasing amount of data is being shared and stored online, the issue of personal and collective privacy presents challenges on an unprecedented level. The fact is that breaches of confidentiality are commonplace. Private conversations between any individual and their friends, family, doctors, lawyers, educators and neighbours are subject to interception by any number of third parties. Those same conversations are subject to government surveillance, often untargeted. Daily activities never considered to have a confidential element, such as buying books, taking a public bus, reading an article, all expose data and details about ourselves that we never knew we needed to hide from others who would use them against us.

All this takes place against the backdrop of internet business models which are fundamentally insecure. Based on current trends it appears that this form of "surveillance capitalism"[13] will only deepen in the coming years. Consider, for example, the Internet of Things, the proliferation of low-cost and insecure connections to the internet of millions of devices (from motor vehicles to fridges to television to so-called wearables) which exponentially increase the availability of data about people and how they live and therefore the risk to their privacy.

There were several concerning and newsworthy incidents in 2017, including leaks and data breaches, that brought to light how unsafe people's data is/are in the hands of others. One example is the case of Uber. It was revealed this year that the personal information (including names, phone numbers, addresses) of 57 million users and drivers were potentially exposed in late 2016. At the time, Uber chose to not reveal the breach but to pay the hackers USD 100,000.[14] In South Africa, around 60 million information records were exposed through lax security and poor information control on a server that appears to have contained data provided by a credit bureau to the real estate industry.[15] In India, there were multiple reports during the year of data breaches involving the biometrics-based identification system Aadhaar. In May 2017, it was reported that the Aadhaar numbers and personal information of as many as 135 million Indians could have been leaked from four government portals due to lack of IT security practices.[16] There were additional reports during the year of government websites inadvertently publishing personally identifiable information, including names, addresses, bank information and Aadhaar numbers, thereby making them available to the general public.[17] In the United States, a breach

10. https://equalit.ie/deflect-labs-report-1
11. https://equalit.ie/deflect-labs-report-3
12. https://equalit.ie/deflect-labs-report-2
13. The term was first used by Shoshana Zuboff. Read more at https://en.wikipedia.org/wiki/Surveillance_capitalism
14. https://www.identityforce.com/blog/2017-data-breaches
15. https://techcentral.co.za/revealed-real-source-sas-massive-data-breach/77626/
16. https://cis-india.org/internet-governance/news/times-of-india-may-5-2017-aadhaar-numbers-of-135-mn-may-have-leaked-claims-cis-report
17. https://inc42.com/buzz/aadhaar-uidai-government, http://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkw1I.html

at the consumer credit reporting agency Equifax compromised the personal information of as many as 143 million residents – almost half the country.[18]

Integrity

Availability, confidentiality and integrity are interrelated. Research on network health by the Open Observatory of Network Interference (OONI), which detects and documents internet censorship, surveillance and traffic manipulation globally,[19] has shed light on availability issues as well as integrity issues when middleboxes and other such mechanisms actively tamper with network information. A middlebox is a computer on the network whose purpose goes beyond network forwarding, such as for security purposes like setting a firewall, or for necessary network operations like traffic routing. But they can also filter, collect or otherwise manipulate traffic. Often research like OONI's is not conclusive – it only shows that something is not right, but without corroboration or admission of purpose by the parties responsible, we can only guess the motivation or even the mechanism.

A very obvious violation of integrity in 2017 is the proliferation of disinformation online. Email hacks and the manipulation of elections through the creation of fake user identities and orchestrated advertising on social networking platforms have dominated US news all year long, but other countries have also had concerns with election-related breaches and disinformation campaigns. The term "fake news" has emerged, unhelpfully, bandied about by politicians in a manner that has very little to do with the actual integrity of information content. Platforms have responded with efforts to allow greater verification of information and sources, but this also presents challenges, particularly to the notion of when and where an internet intermediary crosses the boundary into a publisher of content.

Additionally, not only is information engineered to be inaccurate, but software and systems can also be manipulated. Malware is malicious software that attempts to hide itself and its processes from an infected user. Infectious malware is particularly rampant among users of popular operating systems and spreads easily without the necessary integrity checks in place, such as antivirus or use of trusted sources for download. Malware affects the integrity of systems and users' or operators' controls over those machines and data.

Phishing attacks, which trick users into giving over their authentication details or other sensitive information, are examples of breaches of integrity. Aside from being used to exploit users for commercial purposes, civil society organisations and human rights defenders are the target of phishing attacks in attempts to compromise and undermine their work. Earlier this year, Citizen Lab and the Egyptian Initiative for Personal Rights (EIPR) documented a large-scale phishing attack on Egyptian civil society. According to the report, almost all of the targets identified are also implicated in Case 173, a sprawling legal case brought by the Egyptian government against NGOs, which has been referred to as an "unprecedented crackdown" on Egypt's civil society. Nile Phish operators demonstrate an intimate knowledge of Egyptian NGOs, and are able to roll out phishing attacks within hours of government actions, such as arrests.[20]

Key developments councerning cybersecurity in 2017

2017 was also an eventful year in terms of policy and regulatory developments, at the global, regional and national levels. As cybersecurity incidents became front page news, pressure increased on policy makers and non-state actors to find ways to address cybersecurity threats, both in ways that aimed to protect human rights and in ways that undermined them in the name of security.

In assessing responses to cybersecurity incidents over the course of the year, a trend that stands out almost uniformly is the participa-

18. http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html
19. https://ooni.torproject.org
20. https://citizenlab.ca/2017/02/nilephish-report

tion deficit. A number of normative statements recognise the important contribution and value of including all stakeholders in addressing risks and threats to the security and stability of the internet. For example, the NETmundial Multistakeholder Statement noted in 2014 that "[e]ffectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders" and that "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, the private sector, civil society, academia, and the technical community."[21]

The following year, the UN General Assembly echoed this in the WSIS+10 Outcome Document, which stated:

> We reiterate our belief that a global culture of cybersecurity needs to be promoted and developed and that cybersecurity measures should be implemented in cooperation with all stakeholders and international expert bodies in order to foster trust and security in the information society.[22]

However, whether at the national, regional or global level, to varying degrees, critical voices and expertise were excluded from policy-making processes.

This section aims to highlight some key policy developments that promise to influence 2018, and beyond. While it goes beyond the scope of this document, it is critical to recognise the valuable contributions by the technical and academic communities to human rights-based approaches to cybersecurity issues. For example, the Internet Society (ISOC) has consistently linked security and rights,[23] and the computer emergency response team/computer security incident response team (CERT/CSIRT) communities are establishing trusted networks for exchanging technical expertise to help improve international cooperation on cybersecurity.

Global

Cybersecurity issues were certainly on the radar of the United Nations this year, with indications that the global body will focus further attention on the issue moving forward. The new UN Secretary-General António Guterres highlighted cybersecurity in his first address at the high level opening of the UN General Assembly, characterising it as a leading threat to international security, citing escalating cybersecurity threats, and warning that cyberwar was now more able to disrupt relations between states, as well as the structures and systems of modern life.[24] A recent report by the United Nations Institute for Disarmament Research (UNIDIR) offers a number of suggestions on

21. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; in addition, the UN Human Rights Council resolution HRC/RES/26/13 "Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development;" http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/13
22. http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf
23. Olaf Kolkman, ISOC's chief technology officer, highlighted the "[r]isk that online freedoms and global connectivity will take a back seat to national security" in a blog post published in October 2017: https://www.internetsociety.org/blog/2017/10/approaches-internet-security-cybersecurity-path-forward; in addition, the New York Cyber Task Force released a series of recommendations in September intended to help make "it easier to defend cyberspace without sacrificing the utility, flexibility, and convenience that has made the Internet so essential to our economies and personal lives." Their report, entitled "Building a Defensible Cyberspace", proposes strategies for government, cybersecurity companies, and others who depend on the internet. They call for greater transparency and also for risk-based governance. They stress the need for government funding and collaboration across sectors: https://sipa.columbia.edu/sites/default/files/embedded-media/NYCTF%20 2017-09-28%20news.pdf
24. https://gadebate.un.org/en/72/secretary-general-united-nations

how the UN Secretary-General might advance human rights in the context of cybersecurity,[25] for example, by:

- Supporting the dissemination and socialization of existing and emerging human rights norms, standards, and principles relating to ICTs. The Secretary-General can encourage the relevant UN departments and agencies to work with other organizations and initiatives to ensure that these norms are mainstreamed across the Organization's existing and evolving capacity-building and technical assistance work. To this end, the UN can promote the inclusion of human rights considerations in national cybersecurity strategy development from the outset rather than as an afterthought;
- Advocating for the engagement of core human rights actors in accompanying implementation of these efforts; and encourage globally recognized technology companies and ICT service and product providers to adopt, implement, and promote the principles and standards they publicly claim to espouse;
- Engaging different actors to identify gaps, garner lessons, foster cooperation, and continue much-needed dialogue on the tensions between rights and security and the important linkages between development and security.

Group of Governmental Experts (GGE)

The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) met over the course of 2016-2017. This GGE, the fifth iteration of the group, was mandated by the UN First Committee of the General Assembly to study "existing and potential threats in the sphere of information security" and measures to address them, including "norms, rules, and principles of responsible behavior of states, confidence-building measures, and capacity-building."[26]

Widely regarded for successfully outlining the global cybersecurity agenda and introducing the applicability of international law in cyberspace, the GGE was expected to advance global norms around state behaviour in cyberconflict. The report of the third GGE in 2013 simply and unambiguously stated that "[i]nternational law, and in particular the Charter of the United Nations, is applicable."[27] It also confirmed that the international norms and principles constituting state sovereignty apply "to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory," and that states should prevent their territories from being used by non-state actors for unlawful use of ICT, and respect fundamental human rights and freedoms.[28]

The report of the fourth GGE in 2015 built modestly on this by noting the legal principles of humanity, necessity, proportionality and distinction. This wording is far from a clear acknowledgement that international humanitarian law applies to state actions in cyberspace, though it represents a nod to the core tenets of international humanitarian law. The 2015 GGE also agreed to four norms for peace-

25. http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf
26. Norms are generally understood as "collective expectations for the proper behaviour of actors with a given identity". In international politics, norms "reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States" (source: General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN document A/70/174, 22 July 2015, para. 10).
27. https://www.justsecurity.org/28062/international-law-gge-report-information-security; http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf
28. General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", UN document A/68/98*, 24 June 2013.

time behaviour: states should not interfere with each other's critical infrastructure; they should not target each other's computer emergency response teams; they should assist other nations investigating cyberattacks; and they are responsible for actions that originate from their territory.[29]

This year's GGE represents a step back. The group failed to reach an agreed consensus or issue a report, owing to disagreement on the right to self-defence and the applicability of international humanitarian law to cyberconflicts, contained in draft paragraph 34. Some states reportedly refused to endorse this paragraph, rationalising that affirming the application of the UN Charter principles on the use of force and international humanitarian law would result in the "militarisation" of cyberspace. Others insisted on including the right to apply "countermeasures" in response to "internationally wrongful acts committed through the use of ICTs" which fall below the threshold of the "use of force" in cyberspace. Given the current political climate between, for example, the United States and Russia, it is not difficult to see how this inclusion of countermeasures could risk opening the door further for destabilising conduct.

The deadlock in the GGE means that for the time being, global norms concerning state behaviour in cyberconflict are at a standstill, at least in the intergovernmental space. The Global Commission on the Stability of Cyberspace is attempting to use a multistakeholder approach to developing such norms (see more on this below). The implications of this are that as attacks in cyberspace continue to proliferate, there is no common understanding of how to respond, and to constrain state action, which could leave people exposed to escalating cyberattacks. Until influential powers like China, Cuba, Russia and the United States can find some common ground, it is likely that norms will be pursued in alternative forums, among like-minded actors.

29. https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what
30. https://cyberstability.org/wp-content/uploads/2017/11/call-to-protect-the-public-core-of-the-internet.pdf

Global Commission on the Stability of Cyberspace (GCSC)

The Global Commission on the Stability of Cyberspace is one such forum that is looking to advance norms on cybersecurity in the absence of progress at the UN. This Commission, which began its work in 2017, aims to help "promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity." It is an initiative of the The Hague Centre for Strategic Studies (HCSS) and the EastWest Institute (EWI), with the political support of the Dutch government. It has made some progress. In November 2017 the Commissioners issued a "Call to Protect the Public Core of the Internet". It urges "state and non-state actors to avoid activity that would intentionally and substantially damage the general availability or integrity of the 'public core' of the Internet."[30] According to their definition, the internet domain name system, routing systems and cable infrastructure would form part of this public core.[31]

A "Digital Geneva Convention"

Early in 2017, in response to the increase in cybersecurity incidents around the world, Microsoft proposed its own framework for enhancing security in cyberspace, informally called a "Digital Geneva Convention". In the words of Brad Smith, Microsoft's president and chief legal officer, "Just as the Fourth Geneva Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies."[32]

The three-part proposal includes: 1) an agreement among nation-states to refrain from

31. https://cyberstability.org/news/global-commission-proposes-action-to-increase-cyberspace-stability/
32. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#IejPPCXozVUcstdm.99

cyberattacks; 2) an agreement among industry actors called a Tech Accord, which would create a shared set of principles and behaviours to protect citizens; and 3) the creation of a new, neutral non-governmental organisation that would investigate attacks and attribute them to perpetrators (though not respond to them or enforce compliance).

Although the Digital Geneva Convention is not formally being debated by any intergovernmental organisation, it has created quite a bit of discussion among states and other actors, and Microsoft has presented the idea at high-level forums, including most recently "Peace Week" in Geneva.[33]

Global Conference on Cyberspace (GCCS)

The Global Conference on Cyberspace (GCCS) is the latest incarnation of a series of conferences often referred to as "the London process".[34] An initiative of the UK government, the GCCS aims to advance global norms for responsible behaviour in cyberspace. This year's GCCS took place in New Delhi, the first time it was hosted in the global South.

The overall theme for GCCS was "cyber4all", with four sub-themes: cyber4growth, cyber4digitalinclusion, cyber4security and cyber4diplomacy. The outcome of the conference was a Chair's Statement,[35] despite the intention of the Indian government originally for there to be a "Delhi Declaration", a consensus text presented on behalf of all Conference participants.[36] Conspicuously absent from the Chair's Statement were human rights. There were zero references to the term, and the sole reference to "rights" is heavily qualified: "Freedom with reasonable restrictions in the larger interests of societies and respect for the privacy rights of individuals and groups are prerequisites for creating Cyber Space for all." [emphasis added][37] Civil society participation was highly constricted in comparison to previous years, with limitations on Indian civil society in particular, and where human rights were discussed, conversations were shallow and did not substantively address key issues flagged by civil society ahead of the conference.[38]

International Telecommunication Union (ITU)

As in previous years, a number of cybersecurity-related issues came up in several forms and formats at the International Telecommunication Union (ITU), the specialised UN agency dedicated to information and communication technologies. For example, the ITU's Study Group 20 is developing non-binding Recommendations (i.e. standards) technical papers, and supplementary resources on the Internet of Things (IoT) and smart cities and communities. As in previous ITU meetings, the Digital Object Architecture (DOA) framework was proposed as a solution. DOA is a proprietary technology that suffers from a lack of transparency, and adopting DOA as the framework for coordinating the identification of IoT devices raises serious security concerns.[39]

The World Telecommunication Development Conference (WTDC) held in November became the latest battleground for cybersecurity at the ITU. The last two days of the conference were largely dedicated to resolving different views among delegations on the content of the cybersecurity resolution, and the role of the ITU in addressing issues relating to cybersecurity. Ultimately, an agreement was reached to adopt the previously agreed text from the last WTDC. However, the issue is likely to re-emerge at ITU meetings next year, including its Plenipotentiary Conference, as persisting divisions among

33. https://www.theregister.co.uk/2017/11/10/microsoft_president_calls_for_digital_geneva_convention/
34. https://www.apc.org/en/news/what-global-conference-cyberspace-faqs-gccs-hague-16-17-april-2015
35. https://www.newkerala.com/news/full-news-292117.html
36. https://www.gp-digital.org/gccs2017-a-cyber-space-free-open-and-secure-but-mostly-secure/
37. https://www.accessnow.org/gccs-2017-shallow-conversation-lack-inclusion-limit-success/
38. https://www.accessnow.org/gccs-2017-shallow-conversation-lack-inclusion-limit-success/
39. https://www.article19.org/resources/doa-for-iot-at-itu-t-study-group-20-dead-on-arrival-or-return-of-the-living-dead/

states on the role of the ITU with regard to cybersecurity were not resolved.[40] These divisions range from being legal and technical to political in nature. From a human rights perspective, proposals that seek to, or would have the effect of, controlling content and the flow of information across borders, undermining anonymity, and centralising decision making on cybersecurity matters in an intergovernmental body are of particular concern.

Regional

The Council of Europe Convention on Cybercrime, known as the Budapest Convention,[41] remains very influential and is used as a model in other regions. The African Union Convention on Cybersecurity and Personal Data Protection has not been formally signed and ratified by many countries on the continent. Just one additional government signed the Convention in 2017 (Ghana),[42] which raises questions about its potential to harmonise regional policy, although some governments are drawing on it in developing national legislation.

Efforts at regional level during 2017 seem for the most part to have focused on cooperation and capacity building. In the Americas, in May 2017 the Organization of American States (OAS) established a Working Group on Cooperation and Confidence-Building Measures in Cyberspace. The mandate of the Group, which falls under the Inter-American Committee Against Terrorism (CICTE), is to prepare a set of draft confidence-building measures, based on points of consensus from previous GGEs, to enhance cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation and conflict that may stem from the use of ICTs.[43] The Group is due to meet for the first time in February 2018.

The OAS engaged with stakeholders on cybersecurity issues a few times during the year. For example, in September, the OAS organised the Cybersecurity Symposium for the Americas Region in Montevideo, Uruguay to provide specialised training in cybersecurity for technicians, law enforcement agents, members of civil society, as well as those interested in and responsible for the development of national cybersecurity policies. The following month, a workshop on Cybersecurity and Civil Society in the Americas was held at the OAS headquarters in Washington, DC.

The CICTE also has a mandate to provide technical assistance to OAS member states to better assess vulnerabilities, shortcomings, threats, risks and interdependence for the development of plans for their optimal protection through exchanges of good practices and experiences. Its 2016 Declaration on Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas invites member states to respect human rights in the use of cyberspace, strengthen cooperation among CSIRTs as well as among law enforcement institutions, and develop protocols for communication among member states. [44]

In Europe, the European Commission adopted a new cybersecurity strategy "to further improve EU cyber resilience and response."[45] The new strategy contains some practical measures to increase cross-border collaboration and strengthen the role of the EU's IT security agency European Union Agency for Network and Information Security (ENISA). It also problematically implies that surveillance of each individual's online activities is a goal of cybersecurity policy.[46] Other relevant developments in the EU include the adoption of a position by the European Commission on the

40. https://www.cfr.org/blog/how-cyber-sidelined-development-itus-world-telecommunication-development-conference
41. https://www.coe.int/en/web/cybercrime/the-budapest-convention
42. As of July 2017, just nine states had signed the treaty, and one (Senegal) had ratified it. https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf
43. CICTE Resolution to Establish a Working Group on Cooperation and Confidence-Building Measures in Cyberspace, document OEA/Ser.L/X.2.17/ CICTE/RES.1/17,7 April,2017.
44. http://www.state.gov/p/wha/rls/259346.htm
45. https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
46. https://juliareda.eu/2017/09/state-of-the-cyber/

issue of encryption.[47] Tucked into an "anti-terrorism package", the position appears to resist some of the more extreme approaches of limiting or breaking encryption at random intervals. However, the policy treats encryption as an overall setback for law enforcement authorities, and the European Commission sends a concerning political message by placing its position on encryption in a policy on terrorism. Another relevant development in Europe is a process under way at the Council of Europe to prepare an additional protocol to the Cybercrime Convention – a new tool for law enforcement authorities to have access to data in the context of criminal investigations.[48] In addition to having major implications for the right to privacy and due process, this development is relevant to cybersecurity, as governments resort to hacking to obtain data that they ostensibly need access to in relation to criminal investigations.[49]

Trends in national legislation

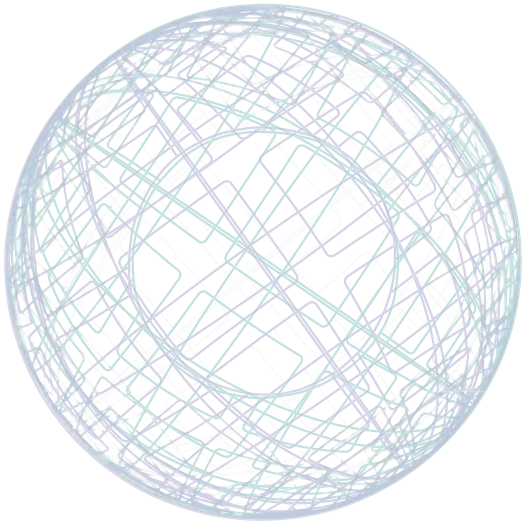
Cybercrime has a significant economic cost, particularly but not only for the financial service industry. There is often a cost for individual users. Governments are, rightly, wanting to respond to threats to "cyberinsecurity", but these responses appear to be, most often, through policies that increase their power to monitor and intercept communications and weaken encryption, rather than by strengthening the security of and providing remedy for individual users. Moreover, these policies are often accompanied by efforts to criminalise freedom of expression and other rights-enabling uses of the internet. Such shortsighted responses fail to protect the rights and security of citizens, in particular those who are most at risk or play essential functions in society, like journalists and human rights defenders.

As previously mentioned, there is a trend of cybersecurity responses being treated as national security matters, and treated with a veil of secrecy, meaning that they are not subject to public debate or scrutiny, and often lack transparency, oversight and accountability. A survey of legislative developments in 2017 is beyond the scope of this brief. However, it is important to note that such shortsighted approaches to cybersecurity are being seen across various regions, from developed and developing governments alike.[50]

Conclusion

The intention of this briefing document is to highlight some key developments in the last year relating to the current climate around cybersecurity and human rights in order to set the stage for a dynamic and in-depth discussion at the Day 0 event. Gaps and shortcomings of this briefing should be discussed and debated on a range of topics, with the goal of identifying rights-based approaches that bridge policy and technical solutions. Anticipated topics for discussion include, but are not limited to, global norm development, confidence-building measures, capacity-building initiatives, government hacking, stockpiling or exploiting vulnerabilities, state-sponsored malware, restrictions on encryption and privacy enhancing technology, conflation of national security and cybersecurity, insecurity of IoT, cyberattacks and cyberespionage used by nation-states and other actors, and cross-border government access to data.

47. https://edri.org/european-commission-struggles-find-position-encryption/
48. https://edri.org/crossborder-access-to-data-has-to-respect-human-rights-principles/
49. https://medium.com/privacy-international/privacy-internationals-work-on-hacking-153a0565e1ce
50. For example, in the UK, Prime Minister Theresa May has threatened weakening encryption https://www.wired.com/2017/06/theresa-may-internet-terrorism; in Kenya, the government is considering a new cybersecurity strategy that would result in more surveillance and less security https://medium.com/@privacyint/surveillance-does-not-equal-security-analysing-kenyas-approach-to-cyber-security-400c73cd93bf



APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS