KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

SECURITY PROPOSALS TO THE ITU COULD CREATE MORE PROBLEMS, NOT SOLUTIONS

September 6, 2012

Member States of the International Telecommunication Union (ITU) are considering this year whether to extend the ITU's regulatory authority to the Internet. Several proposals have been made to revise the ITU's basic treaty to include provisions addressing the security of networks or information. These proposals have rightly raised controversy not only because of their implications for Internet freedom, but also because of concerns that ITU intervention could distract from or undermine other ongoing efforts by institutions better suited to address Internet security.

I. Background on ITU, Internet Governance, and the Security Proposals

The International Telecommunication Union (ITU) is an agency of the United Nations with a specialized focus on telecommunications regulation, as well as radio regulation and development. The ITU's current underlying treaty for telecommunications regulation, the International Telecommunication Regulations (ITRs), was adopted in 1988 and sets forth general principles for the operation of international telephony systems. Member States of the ITU are considering expanding these regulations to Internet matters by amending the ITRs at the World Conference on International Telecommunications (WCIT), scheduled for December 2012 in Dubai, UAE. Several proposals have been offered to expand the ITRs to include issues of cybercrime and cybersecurity.[1]

The ITU's regulatory approach diverges significantly from the lightweight and decentralized type of governance that has sustained Internet development and innovation to this day. Thus far, Internet governance has been conducted by a mix of self-regulatory initiatives, multi-stakeholder organizations, and voluntary technical standards bodies, taking on specific challenges as needed. The proposals on the table at the WCIT, on the other hand, are in many cases so broad and general that they could reach potentially every aspect of the Internet's development. Further, while Internet governance has involved a wide range of stakeholders, including civil society and technical experts, the model of the ITU is government-centric. Although there is some limited opportunity for companies and civil society organizations to participate in some discussions at the ITU as

[1] CDT has previously warned of the risks of expanding the ITU's mandate to encompass issues affecting the Internet. See CDT, ITU Move to Expand Powers Threatens the Internet, https://www.cdt.org/files/pdfs/CDT-ITU_WCIT12_background.pdf https://www.cdt.org/report/itu-move-expand-powers-threatens-internet (March 12, 2012); Cynthia Wong, ITU Discussions Must Be Opened, https://www.cdt.org/blogs/cynthia-wong/1705itu-discussions-must-be-opened (May 17, 2012). We are analyzing other specific proposals that have been put forth to expand the ITRs. See CDT, ETNO Proposal Threatens to Impair Access to Open, Global Internet, https://www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf (June 21, 2012).

Sector Members, governments control its formal decision-making process. And, in practice, the high costs of membership mean that the ITU is made up primarily of Member States and companies.

This paper focuses on the proposed changes to the ITRs concerning security. We first discuss the existing efforts to address complex cybersecurity issues at an international level. We then analyze three specific issues that have been raised in various security-related proposals to amend the ITRs, explaining how these proposals could threaten Internet users' right to privacy and free expression. We then explain why, due to the organization's structure and lack of subject matter expertise, the ITU is not an appropriate entity to take on the complex issue of cybersecurity. We conclude that the ITU is ill-suited to addressing the problem of cybersecurity effectively and that by adopting cybersecurity as part of its mandate it could delay, supplant, or frustrate other more meaningful efforts.

II. Existing International Bodies Are Already Addressing Cybersecurity

The cybersecurity issue is critically important, and a large number of countries have legitimate interests in expanding both international cooperation and their own national responses on the issue.[2] As a complex policy issue, cybersecurity has several defining characteristics: First, effective solutions will be developed only with the participation of a variety of stakeholders, including ICT companies (communications service providers, hardware and software makers, e-commerce companies, and other online services); the critical infrastructures that depend on the Internet; technologists; law enforcement agencies; human rights advocates; and users. Further, given the pace of technological change, governmental bodies are not likely to be the source of effective technical solutions. The issue requires speed and agility: the cybercriminals are highly adaptive, and all those involved in defending networks need to be able to respond rapidly to changing threats. Given privatization, innovation, and competition, and because the private sector is likely to have greater technical expertise than government regulators, cybersecurity must be based on public-private partnerships, where the government does not have the lead role. Finally, the issue requires solutions at various levels, including improving the practices of the private sector, educating users, improving law enforcement cooperation across borders, and promoting improvement in technical standards. The best structures for addressing cybersecurity are likely to be decentralized rather than centralized, multi-stakeholder rather than government-dominated, and voluntary rather than mandatory.

Within this context, there is already extensive work being done by other international bodies with respect to cybercrime, cybersecurity policy, and security standards. A number of these existing groups, which include the Internet Engineering Task Force and the Messaging Anti-Abuse Working Group, operate under a multi-stakeholder model; they are open to all, regardless of nationality or institutional status, and they are less centralized and more agile than the ITU, with the flexibility to respond to dynamic shifts in threats to networks. Participants in these organizations include not only government

[2] See, for example, the June 8, 2012 comments of Toomas Hendrik Ilves, President of Estonia, http://www.president.ee/en/official-duties/speeches/7589-the-president-of-estonia-at-the-international-conference-of-cyber-conflict-8-june-2012/.

officials and corporate representatives but also academics and engineers with substantive expertise in the relevant technical areas.[3] Over the years, these organizations have developed trust among their participants, in part because participants do not represent a governmental interest but rather a technical expertise.[4] Multilateral cybersecurity policy, with its implications for national defense and security, is highly dependent on such trust between engaging entities.

One example of the way in which the global Internet community already acts to respond to cybersecurity threats is the Conficker Working Group. Conficker was a sophisticated botnet "worm." In 2008, it was released on the Internet and rapidly infected millions of government, business, and home computers in over 200 countries. Very quickly, major Internet companies, ISPs, domain name registries, independent technologists, academic researchers, representatives from ICANN, and others from around the world came together and formed the Conficker Working Group. Governments also participated, but governments neither convened nor led the effort. The group rapidly developed and implemented measures that successfully stopped the spread of the worm. There were limits to the Group's effectiveness; in particular, while it stopped the spread of the worm, it was not able to convince computer owners to remove it from most of the computers it had infected. The lessons learned from the Conficker experience deserve widespread attention, but they do not point in the direction of top down, governmental mandates. Instead, they point towards multi-stakeholder partnerships, addressing concrete problems, and working with transparency and inclusiveness.[5]

Regarding the role of inter-governmental bodies in addressing cybersecurity, it is important to note that several such bodies currently provide forums for cooperation on cybersecurity policy. The Council of Europe is one example: its Convention on Cybercrime seeks to provide a framework for addressing cybercrime not only among the Members of the COE, but globally. While the COE Convention on Cybercrime is not a perfect instrument, the COE has developed deep expertise in this area. Despite its flaws, the Convention offers a framework through which countries can cooperate in exchanging information and prosecuting cybercrime. The Convention is open to ratification not only by members of the COE but by all states. Discussion of Internet-related policy and standards also occurs in existing ITU Study Groups, which may develop non-binding recommendations for approaches to dealing with cybersecurity issues.

Rather than seeking to create through the ITRs new authoritative powers within the ITU for cybercrime and cybersecurity cooperation or enforcement, it is best to work through existing structures to improve both responses to cybercrime and the protection of human rights.

---

[3] See http://www.ietf.org/ and www.maawg.org.

[4] See A.M. Rutkowski, W.A. Foster, S.E. Goodman, Multilateral Cyber Security Solutions: Contemporary Realities.

[5] See "The Conficker Working Group Lessons Learned Document"(June 2010, published January 2011) http://www.confickerworkinggroup.org/wiki/.

III. Analysis of Three Security Issues Proposed for Inclusion in the ITRs

The word "security," which does not appear in the existing ITRs, appears multiple times in various proposals offered to amend the ITRs.[6] Other phrases that are used to describe the issues that are proposed to be brought within the scope of the ITRs are "confidence," "trust," "data and network integrity," "information security," "network security," "cybercrime," "misuse of ICTs," "eavesdropping," "breach of privacy," and "data protection." Many of these terms are ambiguous; some have been used by governments in connection with measures that interfere with free expression, openness, and personal privacy. Below, we analyze three specific issues raised by the pending proposals.

A. Proposals to Require Member States to Cooperate to Address Cybercrime

The Arab States regional group has offered a proposal to amend the ITRs to require Member States to "undertake appropriate measures, individually or in cooperation with other Member States" to address issues relating to "Confidence and Security of telecommunications/ICTs," including "***physical and operational security; cybersecurity, cybercrime, and cyber attacks; denial of service attacks; other online crime; controlling and countering unsolicited electronic communication (e.g Spam); and protection of information and personal data (e.g. phishing).***"[7] Several other proposals encourage Member States to cooperate in harmonizing laws related to the investigation and prosecution of cybercrimes crimes, along with other aspects of cybersecurity.[8] While the proposals' cooperation framing is preferable to an

[6] Our analysis here is based on two ITU documents that compile the proposals offered by various countries and regional groups to amend the ITRs: CWG-WCIT12 Temporary Document 64 Rev. 1 – Anticipated Final Draft of the Future ITRs ("TD 64") (18 June 2012), http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLEN-0064!R1!MSW-E.pdf, also available at http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf, and CWG-WCIT12 Temporary Document 62 Rev.2 – Draft Compilation of Proposals with Options for Revisions to the ITRs ("TD 62") (29 June 2012), http://files.wcitleaks.org/public/T09-CWG.WCIT12-120620-TD-PLEN-0062R2.pdf. TD 64 is a "redline" of the current ITRs, compiling all proposed changes as of its date; it includes a proposed new Article 8A that compiles many of the security-related proposals. TD 62 is a chart compiling the comments of various Member States in justification of or opposition to the proposed changes. These documents have been made available through the WCITLeaks.org website and may not be fully up-to-date. Either or both may have been revised or superseded. Indeed, one of the problems with the ITU as a policy-making body is that it does not release most of its documents for public debate.

[7] TD 62, pp. 181-182.

[8] The Africa regional group has proposed that:

"Member states shall cooperate to harmonize national laws, jurisdictions, and practices in the areas of: the investigation and prosecution of cybercrime (including eavesdropping and breach of privacy of telecommunications), data preservation, retention, protection (including personal data protection), and privacy, and approaches for network defense and response to cyberattacks." TD 62, p. 195.

The Study Group 3 Regional Group for Asia-Oceania (SG3RG-AO), along with Algeria, Egypt, and the Russian Federation, proposed language stating:

outright mandate, they all involve the idea that the ITU should be a primary locus for international cooperation in an area raising many concerns for law enforcement and national security as well as for innovation, privacy, and free expression.

As a threshold matter, these proposals underestimate the complexity of the cybercrime and cybersecurity issue. Cyberthreats come from a broad range of sources, from national level actors engaging in theft of state secrets to teenagers hacking into school computers. In the view of the Council of Europe, as expressed in its Convention on Cybercrime, the cybercrime issue itself involves not only crimes *against* computers, but also crimes facilitated by computers and crimes where evidence is transmitted through or stored on computer systems.[9]

On the one hand, if the ITRs were to address cybercrime at a high level of generality, there is the risk that some Member States would cite the ITRs a pretext for intrusive or repressive measures. A provision in the ITRs referring to the need for "greater confidence and security, including of information,"[10] for example, might be used to support laws stifling dissent.[11] On the other hand, to really address the issue in its complexity, the ITU would have to address not only the question of how to define cybercrimes without infringing on free expression, but also how to investigate them while respecting the right to privacy. CDT believes that a global dialogue is needed to develop strong standards, based on human rights principles, to regulate government investigative powers in light of the intrusive potential of digital technology, but we do not believe that the ITU is the right body to conduct that dialogue. And if the ITU is not equipped to enter into the complexities of defining, investigating and prosecuting cybercrimes, it should not open the door by vague references to cybercrime or cybersecurity in the ITRs.

B. Proposal to Require Member States to Cooperate to Harmonize Data Retention Laws

The proposal of the African Member States on security specifically urges Member States to cooperate to harmonize their laws on data retention (the requirement that

---

"Member states shall cooperate to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues. Member states in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness." TD 62, p. 189.

SG3RG-AO and Egypt proposed language stating, "Member states shall cooperate with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime." TD 62, p. 191.

See also TD 62, p. 174, proposal of the Russian Federation and Algeria (text to be defined); TD 62, pp. 179-80, proposal of the RCC on confidence and security.

[9] Convention on Cybercrime, Budapest, 23.XI.2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[10] See TD 62, p. 25.

[11] Countries, of course, already use cybersecurity and national security claims to support repressive measures. Consider, for example, Iraq's law imposing life in prison for intentionally using a computer for the purpose of "undermining the independence, unity, or safety of the country, or its supreme economic, political, military, or security interests." See http://www.hrw.org/reports/2012/07/11/iraq-s-information-crimes-law.

communications companies retain for the benefit of the government data about customers and communications that is not required for business purposes).

This reference to data retention well illustrates the problems with involving the ITU in issues related to cybercrime and cybersecurity. Not only do national laws on data retention vary greatly, but there is ongoing controversy about whether governments should impose data retention mandates at all.[12] In addition, where data retention is required, there are many different views on the legal standards under which governments should be able to gain access to retained data – whether access should require a court order, for example. Such questions are crucial to adopting a data retention law, but are far outside the expertise of the ITU. Other concerns arise from the fact that data retained by a service provider may, absent specific legal and procedural safeguards, be subject to access by the government to investigate any crime, may be accessed by intelligence agencies, and may be shared with other governments to assist their investigations. In addition, the more data that companies are required to retain, and the longer the retention period, the greater the risk that personal information could be breached, leaked, or otherwise abused.

Countries with criminal laws that operate under the presumption of innocence may find that data retention laws turn that presumption on its head, since these laws apply to every citizen regardless of whether they have committed a crime. Further, because data retention laws require service providers to store information that identifies individuals online, they threaten anonymity online, implicating the rights to both privacy and free expression.

For all of these reasons, many countries have chosen to reject legislative data retention mandates. Some countries opt instead for data preservation mandates, which authorize law enforcement officials to require service providers to retain specific data for a period time as the officials proceed with their investigation. In any case, it is clear that there is no one-size-fits-all solution to the question of whether and how to make data available to government actors. The ITU is not equipped to wade into these troubled waters.

C. Proposals to Permit Member States to Impose Restrictions on the Routing of Communications over the Internet and Collect Subscriber Identity Information

Several proposals to amend the ITRs refer to the routing of communications, meaning the path a telephone call – or, potentially, Internet traffic[13] – takes between the sender and recipient.[14] One proposal from the Arab States regional group would amend the ITRs to specify that "A Member State has the right to know how its traffic is routed."[15]

---

[12] CDT, Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development (Oct. 2011) https://www.cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf.

[13] The Internet is outside of the scope of the current ITRs, but proposals to change key definitions, including the definition of "telecommunications," or proposals to make ITU-T Recommendations mandatory that specifically involve Internet-related issues such as naming resources or spam, could change the scope of the treaty.

[14] See TD 62, pp. 87-89.

[15] TD 62, p. 87. An earlier version proposed revising Article 3.3 of the ITRs to state that "A Member State shall have the right to know through where its traffic has been routed, and should have the right to impose any routeing regulations in this regard, for the purposes of security and countering fraud."). TD 62, p. 88.

The proposal is justified on the grounds of security, which some Member States clearly interpret to mean national security. In its comments, Egypt argued, "There must be transparency of the routes: on request, Member States must be able to know the routes used, in particular to avoid fraud and to maintain national security. If the [Member State] does [not] have the right to know or select the route in certain circumstances (e.g. for Security reasons), then the only alternative left is to block traffic from such destinations, which is neither logical nor desirable!"[16]

A number of countries have raised concerns over fraudulent international telephone call diversions, which affect the international charging and settlement scheme, and in that context the Arab States' proposal and others relating to routing and identification may make a certain amount of technical sense.[17] In simplified terms, telephone communications are conducted over circuit-switched networks, which establish a dedicated link or circuit between the two endpoints of a call. In that context, it is at least technically feasible to know, and control, the route that an entire communication takes.

However, Internet protocol (IP) networks transmit communications and interconnect entirely differently than traditional telephone networks; in that context the Arab States proposal to "know how traffic is routed" simply would not work and could fundamentally disrupt the operation of the Internet. When a communication is sent over an IP network, it is broken up into packets, each of which could potentially take a different path across a series of interconnected networks as it journeys to the recipient. A single packet could potentially route through networks hosted in a number of countries before landing at the recipient's computer, all without the control or even knowledge of the sender or recipient. If the Arab States proposal were applied to all Internet communications, the requirement that countries be able to "know" how every IP packet is routed to its destination would necessitate extensive network engineering changes, not only creating huge new costs, but also threatening the performance benefits and network efficiency of the current system.

The Arab States proposal could also serve to legitimize, by enshrining in an international treaty, governmental efforts to establish controls on Internet traffic. Changes to IP routing procedures to implement the Arab States proposal could give Member States additional technical tools to use to block traffic to and from certain websites or nations. The regulations on routing that the Arab States proposal condones could take a variety of forms, from prohibiting certain IP addresses from being received inside a country to tracking users by IP addresses and blocking specific individuals from sending or receiving certain communications. "Knowledge" of IP routing could also encompass countries keeping track of what websites their citizens visit or with whom they email – all in the name of national security. These types of regulations, which could be legitimized if the Arab States proposal is adopted, could threaten user rights to privacy and freedom of expression on the Internet.

---

[16] TD 62, p. 87.

[17] See, e.g., Geoff Huston, CircleID, Number Misuse, Telecommunications Regulations and the WCIT, http://www.circleid.com/posts/number_misuse_telecommunications_regulations_and_wcit/.

Other proposals would address calling party or origination identification, specifically citing security concerns.[18] For example, one proposal from Russia would require governments to "ensure that operating agencies duly identify the subscriber when providing international telecommunication services, and shall ensure the appropriate processing, transmission and protection of identification information in international telecommunications networks."[19] Again, in the telephony context, these proposals may make sense, but when applied to the Internet they pose fundamental risks to human rights as well as being potentially incompatible with various legitimate services. As most recently articulated by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, the right to privacy is essential for the exercise of the right to freedom of expression. Permissible limitations on the right to privacy must respect the principle of proportionality. Yet we see little evidence that proposals that could limit the right to privacy and freedom of expression have been subject to such analysis under the human rights framework.[20]

IV. ITU is Not the Appropriate Entity to Address Cybersecurity

Cybersecurity as both a policy matter and a technical matter is very complex, involving a wide variety of threats and targets. Not only does the ITU lack the substantive expertise to address these issues, but its formal organizational structure and government-centric membership do not support the kinds of solutions needed to address cybersecurity challenges. Rather, other existing international organizations steeped in technical expertise and open to the participation of a diverse array of stakeholders are better able to achieve solutions at the international level.

A. ITU Organizational Structure and Membership

The ITU is a formal affiliate of the UN with 193 Member States. Its underlying treaty for telecommunications, the ITRs, focuses on regulatory issues for traditional telephony systems and not on the Internet, computing resources, or information processing. While the ITU-T, the ITU's telecommunication standards arm, has developed a variety of voluntary recommendations through its Study Group system, it does not play a strong role in setting standards that are relevant to the security of networks.

Under the current ITRs, ITU action on any given telecommunications topic generally will take the form of high-level principles. The ITU is not designed to get consensus to act quickly in response to a specific, fact-intensive threat such as cybersecurity, to understand the technical details of any particular problem, or to persuade private actors (which own and operate much of the Internet's infrastructure) to cooperate in response.

[18] TD 62, pp. 69-73, 95-103.

[19] TD 62 rev2, pp. 181 (new Article 8.8).

[20] Report of the Special Rapporteur on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet, A/HRC/17/27 (2011), available at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx.

B. Consideration of Human Rights Issues

Cybersecurity issues inevitably involve questions of government surveillance, privacy, free expression, and the free flow of information. The cybercrime and cybersecurity proposals before the ITU, however, fail to address privacy, free expression, and the right to access information, or to propose anything close to adequate safeguards for these key human rights. This may not be surprising, given that the ITU has not historically dealt with issues of fundamental human rights. But the fact remains that the ITU does not have the expertise or experience to do the complicated yet essential balancing between promoting security and preserving liberty that cybersecurity policymaking requires. A pronouncement In the ITRs on one half of the equation (security) without addressing the other half (liberty) could tip the balance in highly undesirable ways. Not being able to strike the balance, it is better for the ITRs not to take on the issue at all.

V. Conclusion

Cybersecurity is a serious challenge to countries around the world, and it is understandable that governments are looking at a variety of venues for solutions. However, making cybersecurity a part of the ITU's treaty would distract from the efforts already underway by other international bodies more capable of addressing various cyber threats. Some of the proposals to amend the ITRs, while seemingly innocuous in their calls for Member States to coordinate steps to improve network security, could be used as justification by some countries to pass laws or regulations that threaten Internet freedom. Rather than amending the ITRs to include references to cybersecurity, we should focus on strengthening the consensus-driven multi-stakeholder models under which the Internet has developed and continues to flourish.

For further information, contact Emma Llansó, Policy Counsel, ellanso@cdt.org, or Jim Dempsey, VP for Public Policy, jdempsey@cdt.org.