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

ITU CYBERSECURITY PROPOSALS THREATEN EXISTING SECURITY EFFORTS, INTERNET OPERATIONS, AND HUMAN RIGHTS

October 4, 2012

This December, the International Telecommunication Union (ITU) will be amending its telecommunications treaty, the International Telecommunication Regulations (ITRs). While the ITRs have played an important role in promoting interoperability and interconnection of traditional telecommunications systems, a number of the proposed revisions would expand the ITRs to include issues of Internet policy, including cybercrime and cybersecurity. The inclusion of security-related measures in the ITRs could have negative consequences for existing multi-stakeholder approaches to cybercrime and cybersecurity, for the technical functioning of the Internet, and for Internet freedoms and human rights.

Cybersecurity Proposals Pending before the ITU Are Too Broad

The security-related proposals pending before the ITU seek to:

- Insert new references in the ITU treaty to cybercrime and cybersecurity.
- Encourage cooperation among the Member States to combat cybercrime.
- Harmonize laws on data retention and on the investigation and prosecution of cyber-crimes.
- Permit Member States to impose restrictions on the routing of communications over the Internet and to collect subscriber identity information.

Key Points

- The word “security” does not appear in the current ITRs.
- The cybersecurity proposals pending before the ITU legitimately reflect the importance of cybersecurity and the imperative of expanding both international cooperation and national responses.
- However, the proposals do not account for the complexity of the cybersecurity issues.
- Given the rapidity with which cybersecurity threats evolve, and because much of the Internet’s critical infrastructure is privately owned and operated, treaty-based bodies such as the ITU are not the ideal source of technical solutions.
- Instead, effective solutions to the cybersecurity threat will only be reached through multi-stakeholder processes involving technical experts, academics and human rights advocates as well as government officials and network operators.

- Making cybersecurity a part of the ITU's treaty would distract from the efforts already underway by other international bodies more capable of addressing cybersecurity concerns and developing security standards, including such governmental efforts as the Council of Europe Convention on Cybercrime (Budapest Convention), non-governmental, voluntary standards bodies such as the Internet Engineering Task Force, and specialized multi-stakeholder coalitions like the Conficker Working Group
- Cybercrime and cybersecurity issues impact free expression and privacy.
- 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 and human rights.
- A number of proposals seek to impose restrictions on the routing of Internet communications. Such control is contrary to the way the Internet works and would require significant reengineering. It could also be used to block traffic and identify subscribers, threatening human rights.

Conclusions

- While greater cooperation on cybercrime is surely desirable, the ITU has little expertise in these issues. The proposals to insert into the ITRs high-level references to cybercrime cooperation underestimate the complexity of the problem.
- ITU intervention on cybercrime and cybersecurity could delay, supplant or frustrate other meaningful efforts already underway in a variety of intergovernmental and multi-stakeholder institutions.
- The risk of negative consequences is compounded by the breadth of terms the proposals use in reference to security, from cyber-attacks to online crime to protection of information and personal data – concepts that clearly go beyond telecommunications and reach into areas of national security and human rights.
- Proposed measures on traffic routing would require extensive network reengineering, likely disrupt the operation of the Internet, and possibly increase the tools with which countries can block traffic and limit freedom of expression and human rights.
- Rather than amending the ITRs to include references to cyber-security, all stakeholders – including the ITU – should focus on strengthening the consensus-driven multi-stakeholder models under which the Internet has developed and continues to flourish.

Further Information

For a fuller discussion of these issues, see "Security Proposals to the ITU Could Create More Problems, Not Solutions," CDT (September 2012), https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf

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