



CENTER FOR DEMOCRACY
& TECHNOLOGY

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

Internet Governance Forum – Workshop 123
Legal Aspects of Internet Governance:
International Cooperation on Cyber-security

RESPECTING HUMAN AND CIVIL RIGHTS IN THE CONTEXT OF CYBERSECURITY

November 15, 2010

John Morris
General Counsel, CDT



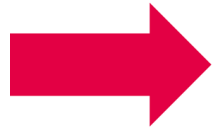
Citizens' Interest in Cybersecurity

- Cybersecurity is not just a governmental or industry concern
 - Citizens' personal business has moved online
 - Identity theft, phishing attacks
 - Internet access is an essential tool for many
- But citizens are also concerned about protecting:
 - Their privacy
 - Their right to speak
 - Their right to due process



Government-Imposed Mandates Should Be Avoided

- Cybersecurity calls for subtle solutions, focused on actual risk in specific sectors
 - Power grid control vs. social networking
 - Solution to one problem should not dictate broader requirements
- Design mandates and “one-size-fits-all” security requirements are problematic
- Private networks should have responsibility for own network security



Problems with Cybersecurity Mandates

- Bad for innovation
 - Mandates raise barriers to new ideas and products
- Bad for competition
 - Mandates raise barriers to entry to markets
 - Only larger well-established players can afford to comply with mandates
- Bad for security
 - Government does not have monopoly on smart people
 - Industry can design defenses to specific risks
 - Industry can quickly respond to new risks



Governments Must Follow Law in Responses to Cybersecurity Threats

- Governments must protect their own networks from attack
- But they must also be sensitive to the human rights of their citizens
 - Privacy
 - Free speech
 - Due process and judicial review
- Should not use cybersecurity as a pretext for Internet regulation or restrictions
 - Seizing computers of dissidents, opposition



Case Study: ISP Responses to BotNets

- Responding to botnets and zombie computers
 - Australia, Japanese, German, and now U.S. efforts
 - Working Group 8 of the U.S. Federal Communications Commission's Computer, Security, Reliability & Interoperability Council
- Developing industry “Best Practices”
- Very careful about risks to consumers, users
 - Detection of compromised computers
 - Privacy risks, DPI
 - Response to compromised computers, attacks



CENTER FOR DEMOCRACY
& TECHNOLOGY

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

Questions?

John Morris
Center for Democracy &
Technology

jmorris@cdt.org