CYBERCRIME

GOALS AND PRIORITIES

- Promote widespread adoption of the Budapest Convention and harmonization of national laws with its provisions
- Build the capacity of countries to combat cybercrime

"The United States is working with partners on every continent to strengthen the capacity of governments to prevent cyber-crime through improved training, the right legal frameworks, information sharing, and public involvement. The best vehicle for international cooperation in this field is the Budapest Convention on Cybercrime, which my government urges every nation to consider joining. There is no better legal framework for working across borders to define what cybercrime is and how breaches of the law should be prevented and prosecuted."

— Secretary Kerry, An Open and Secure Internet: We Must Have Both, Korea University, Seoul, Republic of Korea, May 18 2015.

CONTEXT

Just as the Internet's growth has provided unprecedented opportunities for participation in the global economy and for personal expression, so too has it opened up new avenues for criminal activity. Transnational cybercrime is an expanding problem. It includes crimes directed at computers, such as hacking or denial of service attacks. It also includes crimes in which information technology is an integral part of the offense, such as online fraud, identity theft, and the distribution of child exploitation materials.

The cost of cybercrime is enormous. The United Nations Office on Drugs and Crime (UNODC) estimates that identity thieves steal $1 billion per year globally. By another estimate, online retailers lost $3.5 billion as a result of fraud in 2012. A recent report by the Center for Strategic and International Studies estimated that cybercrime and intellectual property theft cost the U.S. economy as much as $100 billion per year. Impossible to measure, however, is the economic cost of reduced trust in the Internet that results from online crime.

To effectively fight transnational cybercrime, national governments need to put in place appropriate laws and develop specialized investigative, prosecutorial, and judicial capacities. Moreover, countries need to strengthen their cooperation by harmonizing their laws and developing means for sharing information and evidence.

U.S. foreign policy focuses on supporting all of these efforts. Central to U.S. policy is the Budapest Convention on Cybercrime, which 47 countries, including the United States, have ratified. The Budapest Convention aims to: (1) ensure law enforcement agencies have the authorities and tools to fully investigate cybercrime and deal with electronic evidence; (2) enact and harmonize substantive cybercrime laws; and (3) create formal and informal mechanisms to ensure effective and timely international cooperation.

CYBER DIPLOMACY

In its bilateral engagements, the United States encourages countries to accede to the Budapest Convention and to harmonize their laws with the provisions of the Convention. To further this objective, the United States supports capacity building through both bilateral and multilateral engagements. To date, 47 countries have become parties to the Budapest Convention and more than a dozen others are in the accession process. The United States also supports the Group of Seven (G7) 24/7 Network, which provides investigators in 70 countries with points of contact in participating countries in order to obtain urgent assistance with investigations involving electronic evidence. In addition, for more than ten years, the United States has supported cybercrime-focused capacity building work as part of its diplomatic and development activities. This capacity building work has focused both on helping countries develop appropriate laws to allow for the prosecution of cybercrimes and training individuals within the criminal justice system on how to investigate, prosecute, and adjudicate cybercrimes consistently and fairly. U.S. multilateral diplomatic engagements have focused on supporting the work of multilateral institutions to provide capacity building for individual countries.

THREATS RELATED TO CYBERCRIME

If the international community fails to improve cooperation in the fight against cybercrime, criminal activity online will continue to grow, with criminals flocking to jurisdictions where enforcement is the weakest. This will be more likely to happen if countries fail to implement comprehensive cybercrime legislation, develop effective high-tech crime investigative capabilities, or are unable to effectively utilize international cooperation mechanisms. Another risk is that certain countries will use valid concerns about cybercrime to violate human rights and promote their broader, and negative, vision for the Internet. The result could be greater fragmentation of the Internet as more countries adopt a state-centered governance model that does not include adequate protections for freedom of speech and political dissidents online.

Office of the Coordinator For Cyber Issues (S/CCI)
United States Department of State

DESIGNED AND PRINTED BY A/GIS/GPS
AUGUST 2015