6th Session of the Intergovernmental Expert Group (IEG) on Cybercrime
July 27-29, 2020
Vienna, Austria

Agenda Item 3: Prevention

U.S. Intervention on Prevention

The Draft Study highlights the importance of cybercrime strategies, which are "important for ensuring that national law enforcement and criminal justice responses fully take into account both the particular challenges of cybercrime, as well as electronic evidence components of all crimes." Despite the importance of these strategies, many Member States lack a comprehensive national cybercrime strategy, including national legislation or policy for cybercrime prevention.

National cybercrime strategies

Top areas of focus for national cybercrime strategies include cybercrime prevention, public-private partnerships, criminal justice capacity, and awareness raising. Notably, cybercrime prevention also requires political leadership and resources for coordinating government initiatives for critical infrastructure. Equally important is political leadership for public-private partnerships. It is frequently noted that in market economies, the great majority of cyber "assets" are held privately. As a consequence, cooperation and information-sharing between government and private industry, and among industry participants, are significant building blocks of anti-cybercrime efforts. Furthermore, published court decisions to inform the public of legal developments are an important transparency tool that raises awareness of how the law is applied in the rapidly changing area of cybercrime.

Capacity-building

"Criminal justice capacity" is another essential area of focus in a national cybercrime strategy. Domestically, the United States conducts frequent training for federal and local prosecutors on the developments in U.S. law and cybercrime investigative best practices. Judicial institutes and conferences also train federal judicial officers on electronic evidence and trial practice. In addition, key federal criminal investigative agencies include special agents who specialize in cybercrime. These agents are supported by computer scientists and other forensic specialists in cybercrime investigations. Internationally, the United States is a

donor to the UN Office on Drugs and Crime ("UNODC") Global Program on Cybercrime and the Council of Europe GLACY+ programs, which provide training to develop and strengthen anti-cybercrime capacity around the world. The United States also maintains its own training programs in Latin America and the Caribbean; Asia; and Africa to share expertise and to enhance cooperation on cybercrime. To support its international efforts, the United States has also deployed prosecutors to regional posts around the world and in Washington, DC.

Political support

Institutions in developing countries, including law enforcement agencies and the judiciary, may not be well-resourced and suffer from a capacity shortage. This shortage affects cybercrime investigation, and as a result, international cooperation, across all law enforcement issues in cybercrime: prevention, investigation, prosecution, and adjudication. It is particularly important not to detract from both the political will and financial resources for ongoing capacity building efforts. As the Draft Study suggests, and as has been reaffirmed in several subsequent UN Commission on Crime Prevention and Criminal Justice ("CCPCJ") and UN General Assembly resolutions, Member States agree that assistance to developing countries to strengthen capacity should be an international priority. To that end, the United States is pleased to be a major donor to the UN Global Programme on Cybercrime.

Collaboration on cybersecurity is distinct from programs to support cybercrime investigations. Although often seen as two sides of the same coin, cybercrime enforcement in the United States is uniquely a government responsibility whereas cybersecurity is the responsibility of a range of public and private actors. Furthermore, public and private organizations continue to promote awareness-raising among businesses with programs intended to improve the cybersecurity skills of mission-critical business information technology staff.

Importantly, as Member States develop wide-ranging strategies for cybercrime prevention, countries must be mindful of their international human rights obligations. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has called the Internet "an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress…" As the Special Rapporteur also went on to say, "[F]acilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States."