

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime & Terrorism
April 12, 2011

(Weinstein) Definition of Cybersecurity In International Law

Mr. Weinstein, our nation has a unique opportunity to take a strong leadership role in defining Cybersecurity in international law. What are the steps that the Justice Department is taking to define Cybersecurity in international law?

Answer:

The Department of Justice agrees that the United States should take a leadership role in forging consensus regarding international law as it pertains to cyberspace. Building on existing norms, legal principles, international agreements, and domestic law, we believe that the United States has an opportunity to build shared understandings regarding international law as it pertains to cyberspace in a positive way that fosters innovation, promotes freedom of expression, and prohibits malicious cyber activity. As discussed below, numerous elements of the United States Government have important roles to play in the development of international cyber law.

Cybersecurity (a subcategory of international cyber law) is a broad concept that encompasses many disciplines and agencies of the United States Government. The Department of Justice is an important component in protecting our nation's cybersecurity, but our efforts in this area involve collaboration with the Departments of Homeland Security, Defense, State, Commerce, and several others.

The Department is working with our interagency partners to lead and develop international consensus in each aspect of cybersecurity.

To carry out the Department's primary responsibility, the promotion of effective investigations and prosecutions of cyber-offenders, the Department continues to take a leadership role in promoting the Budapest Convention (Council of Europe Convention on Cybercrime), which the Department helped negotiate and worked with the Senate to ratify in 2007. The Convention pioneered the international definition of key cybercrimes and the tools necessary to investigate crimes committed using computers and networks.

The Department continues to work with our international partners to build their law enforcement and prosecution capacities. We use State Department Foreign Assistance funds to provide capacity-building training and technical assistance to developing countries, including advice on developing their legal frameworks in this area.

Due to the transnational nature of most cybersecurity incidents, achieving effective multilateral cooperation in real time has become a priority. The Department actively promotes tools for international law enforcement cooperation and information sharing, such as the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid

law enforcement coordination across borders.

Senator Sheldon Whitehouse
U.S. Senate Judiciary Committee
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime & Terrorism
April 12, 2011

Question to Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice; Gordon Snow, Assistant Director, Cyber Division, Federal Bureau of Investigation; and Pablo Martinez, Deputy Special Agent In Charge, Criminal Investigation Division, Cyber Crime Operations, United States Secret Service. Per my request at the hearing, please describe the extent to which your organization's cyber security resources are empowered to supplement criminal enforcement efforts with the use of civil injunctive tools to combat cyber security threats.

Answer:

Given the increasingly complex threats we face, the Department uses both civil and criminal authorities to counteract a variety of online crimes. Most recently, on April 13, 2011, the Department combined civil and criminal statutory authorities in an effort to disable the Coreflood botnet in the most comprehensive enforcement actions ever taken by U.S. authorities against an international botnet. The operators of the botnet surreptitiously spread malicious software to hundreds of thousands of computers across the United States. Among the functions of the botnet was code that silently captured private communications and financial information of victims. In that case, the Department announced the filing of a civil complaint, the execution of criminal seizure warrants, the issuance of civil forfeiture seizure orders for domain names, and the issuance of a temporary restraining order and later a preliminary injunction. The U.S. Attorney's Office in Connecticut filed the civil complaint against 13 John Doe defendants, alleging that the defendants engaged in wire fraud, bank fraud, and illegal interception of electronic communications. In addition, search warrants were obtained for computer servers throughout the country, and civil seizure warrants were obtained in the U.S. District Court for the District of Connecticut for 29 domain names. Finally, the government obtained a temporary restraining order, authorizing the government to respond to signals sent from infected computers in the United States in order to stop the Coreflood software from running. This action prevented further harm to hundreds of thousands of unsuspecting users of infected computers in the United States. This action was taken in close consultation with computer security and industry experts.

The Department will continue to be creative and aggressive in using appropriate and lawful tools – both civil and criminal – to bring down botnets and other forms of serious international cyber crime.