

Before the United States Senate Judiciary Committee, Subcommittee on Crime and Terrorism
“Cyber Security: Responding to the Threat of Cyber Crime and Terrorism”
April 12, 2011

Responses to Questions Submitted by Senator Orin Hatch
By John E. Savage

International Cooperation

Professor Savage, in your prepared statement you advocate for exploring proposals for effective international cooperation on the development of cyberspace norms and rules of the road. I believe that a strong cyber policy should be a topic of discussion in trade agreements and included in economic and foreign policy strategies when we engage foreign nations in diplomacy.

1. In order to gain effective international cooperation, do you believe that enforcement of the rule of law in cyber crime should be included into trade agreements?

Because I have only a general layperson’s knowledge of trade agreements, I do not have an expert opinion on the role that the rule of law on cyber crime should have in such agreements. However, I am sufficiently knowledgeable about the Council of Europe Convention on Cybercrime (CoC) to appreciate that it can help to understand the value and efficacy of treaties that do require adherence to the rule of law on cyber crime.

The CoC advertises itself as “the only binding international instrument dealing with cybercrime.” It is designed to a) harmonize national laws on cybercrime, b) improve national capabilities to investigate such crime, and c) enhance international cooperation in this area.

Its effectiveness may be judged by the fact as of April 25, 2011, 30 countries have ratified the convention. While my personal knowledge of the effectiveness of CoC is limited, the experience of federal law enforcement agencies with the agreement is informative. Deputy Assistant Attorney General Jason Weinstein, a member of the first panel, testified that the Department of Justice relies on the CoC “to provide a framework for efficient cooperation among nations involving electronic crime.”

I take this as a strong endorsement of the effectiveness of insisting on enforcement of the rule of law concerning cyber crime when developing international agreements.

2. Any thoughts on how best we can determine which countries are countries of concern?

During my year in the U.S. Department of State as a Jefferson Science Fellow I learned that the U.S. government makes assessments of which countries are of concern in the cyber arena. This information should be available to the committee in the appropriate forum.

It is often said that a very large fraction of the information that forms the basis for intelligence assessments is available in the general press. Thus, major news outlets, such as the Washington Post, the New York Times, and Reuters, can provide reports that can help to identify countries of concern. A recent Reuters article¹, which

¹ [Special Report: In cyberspy vs. cyberspy, China has the edge](#), Reuters, April 14, 2011.

quotes many authoritative American sources, argues that China is a major threat to the U.S.. Reports of the U.S.-China Economic and Security Review Commission also speak to this issue.

International Definition of Cybersecurity in International Law

Professor Savage, our nation, has a unique opportunity to take a strong leadership role in defining Cybersecurity in international law. I concur with the sentiments of your statement the United States should promote the acceptance of Cybersecurity legal definitions and rules of the game. These should be beneficial to the United States and promote international cooperation.

1. What international body or convention do you believe should be the guardian of Cybersecurity agreements and definitions at the international level?

At the moment there is no one international body or convention that is an acceptable guardian of cybersecurity agreements and definitions. Some members of the International Telecommunication Union (ITU) would like it to play that role, although many in the U.S. are opposed to that proposition. Observing this landscape, the authors of two recent reports described below, while expressing serious reservations about the ITU, nonetheless express alarm that the U.S. is not adequately engaged in international discussions of cybersecurity and Internet governance.

In a September 2010 report² for the Council on Foreign Relations, Robert Knake wrote that, because we have not been fully engaged, the U.S. is being outmaneuvered in those international forums that determine the future of the Internet by countries who favor state control of the Internet. He says that the best way to encompass all the issues and the players involved in cyber security is to “nurture a range of forums – some multilateral, some bilateral, and some regional – to tackle these challenges.” This would avoid state-centered control of the Internet, which he finds unsatisfactory and characteristic of the ITU. He cites the Financial Action Task Force established in 1989 by the G7 as an example of an international body that might be emulated.

In a recent article³ Sofaer, Clarke and Diffie echo the urgent need for the U.S. to engage other nations in negotiating international agreements. They describe three general preparatory steps that have been effective in striking agreements in the past. They are to a) determine the topics that a nation wants included and excluded from agreements; b) define the measures it wishes be incorporated into agreements, such as declarations, information sharing, prohibitions, punishments, cooperation, and standards and practices; and c) the types of administrative structure and allocations of authority that it would like to see in agreements. For each step they describe the issues that they believe are important to the U.S. They close by acknowledging the difficulties and uncertainties involved in striking international agreements.

Before engaging in international cybersecurity agreements, the U.S. government must develop a coherent national cybersecurity strategy, which it should do in conjunction with the public and private sectors.

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I’ve been following this issue very closely and would appreciate learning your views on some the legislative proposals that are pending?

² [Internet Governance in an Age of Cyber Insecurity](#), Robert Knake, Report No. 56, Council on Foreign Relations, September, 2010.

³ [Cyber Security and International Agreements](#), Sofaer, Clark and Diffie, **Procs. Workshop on Detering CyberAttacks**, National Academies, Press. 2010.

1. What are some of the issues we should avoid and others we should embrace?

S. 773, the Cybersecurity Act of 2010, introduced in the 111th Congress, is an excellent bill. It highlights the need to identify critical infrastructure sectors of the U.S. economy, outlines steps to develop a cyber aware and educated workforce, defines the cybersecurity responsibilities of the executive branch in both domestic and international arenas, highlights the need to educate the general public as well as university students, identifies areas for public-private collaboration, provides funding for research in critical cybersecurity areas and calls for the incorporation of cybersecurity into the curricula for industrial control system engineers.

The bill also speaks to the need to certify and accredit cybersecurity degree programs. Unfortunately, it is too early to do that. Top computer science departments typically offer zero or one course on computer security and possibly one or two courses on cryptography. Thus, universities need to be encouraged to introduce cybersecurity course sequences in computer science departments, not just in industrial control curricula.

An attractive feature of S. 3155, the International Cybercrime Reporting and Cooperation Act, introduced in the 111th Congress is the requirement that assistance be provided to UN nations that have a low level of development or utilization of information and communications technologies in key industries. That type of support will win over developing nations whose support we need in the ITU. The bill also would require the President to provide help to “countries of concern” to improve their capacity to combat cybercrime. While laudable, I doubt that such countries will want to cooperate after being identified as a country of concern. It would be better to fund studies in the U.S. on steps that might be taken to encourage the desired behavior. A good example of a productive move that should be further encouraged is the set of talks sponsored jointly by the U.S. Center for Strategic and International Studies (CSIS) and the China Institutes of Contemporary International Relations (CICIR). My understanding is that these talks have brought together private and governmental U.S. representatives to meet with their Chinese counterparts. This form of informal diplomacy may prove to be very productive.

S. 413, the Cybersecurity and Internet Freedom Act of 2011, introduced in the 112th Congress would create the Office of Cyberspace Policy in the Executive Office of the President. The U.S. very much needs to develop a national cybersecurity strategy. This bill imposes a large range of demanding responsibilities on the office and probably will require a large staff. If the new office is to replace the Cybersecurity Coordinator’s Office (approximately seven staff), it is not likely that it can satisfy its mandate.