HLS Hosted Panel of Cybersecurity Experts Discuss Cyberterrorist Threat

Harvard National Security Journal. Volume 2, Issue 2. Nov 2, 2009.

http://harvardnsj.com/2009/11/cybersecurity-experts-discuss-cyberterrorist-threat-at-hls/

By Mat Trachok, HLS 2012 NSJ Staff Writer

What exactly is the nature of the cyberterrorist threat? How realistic is the prospect of nation-to-nation cyberwarfare? How should the government respond to and protect against such threats? What role should the law play in fighting cyberterrorism? On Wednesday, October 28th, the Harvard Law School National Security & Law Association and the Journal on Law & Technology co-hosted a panel discussion moderated by HLS Professor Phil Malone that sought to answer these questions. The panel brought together experts from both inside and outside the U.S. government, including Leonard Bailey, cyberterrorism expert in the Department of Justice National Security Division; Dr. Andrew Colarik, cyberterrorism expert and author; and Kim Taipale, executive director of the Center for Advanced Studies in Science and Technology Policy.

The panelists first addressed how technology has made the United States more vulnerable to terrorists operating in cyberspace. Taipale identified two main weaknesses. He first posited that advances in technology encourage the United States to pursue greater efficiency in the operation of its information systems. Improved efficiency, however, has made the country's infrastructure more fragile: the United States has removed redundancies and created single points of failure in its essential systems. Second, current technology allows small groups and individuals to leverage power that previously could only be leveraged by nation-states. Colarik agreed, saying that cyber attacks offer terrorists and nations the opportunity to inflict extraordinary damage at minimal cost. Indeed, cyberterrorists could cheaply exert control over many essential components of the national infrastructure, including traffic lights, electrical grids, navigation systems, the electronic financial system, and even hospital blood-type registries. Such attacks could not only inflict casualties, but also create widespread chaos by undermining confidence in those systems.

The panelists also discussed how the United States could better protect itself from cyber attacks. Bailey focused on the need to create a lexicon with which to discuss cyber threats, since the inability to discuss them in a uniform way hampers the United States' response capacity. For instance, Bailey pointed out that there is no consensus as to whether a cyber attack carried out exclusively over computer systems is a use of force that triggers Article 51 of the United Nations Charter. Taipale argued for an update to the national security command structure. He maintained that responses to national security threats remain bifurcated even as the threats themselves are becoming increasingly unbounded. Taipale further pointed out that while many approach national security through either a military or a criminal paradigm, most modern threats involve both military and civilian infrastructure (e.g., telephone and missile systems often run through the same systems).

One point of disagreement among the panelists was over Colarik's idea to institute a two-year statutory shelf life on personal data. Currently, personal information is stored on the Internet indefinitely and is

often easily available to terrorists who use it to assume new identities and move with ease across borders. By putting a shelf life on personal information, Colarik argued, it would be more difficult for terrorists to access and use that information. Taipale and Bailey said that while such a measure might improve security, it would necessarily infringe upon the ability of web sites like Google to provide access to a wealth of information, an undesirable consequence.

President Obama named October to be the National Cybersecurity Awareness Month, with the launch of the new U.S. Cyber Command and the opening of the National Cybersecurity and Communications Integration Center (NCCIC). For more on the debate over U.S. cybersecurity measures, see the proposals being discussed today at a symposium hosted by George Washington University's Homeland Security Policy Institute and the Intelligence and National Security Alliance.