What is cyberterrorism? Even experts can't agree
By Victoria Baranetsky
Harvard Law Record, 5 November 2009
http://www.hlrecord.org/news/what-is-cyberterrorism-even-experts-can-t-agree-1.861186

Cyberterrorism is a buzzword that has been thriving in the administration of President Barack Obama '91, but it has such a nebulous meaning that it managed to elude three expert panelists last Wednesday.

Leonard Bailey was transferred from the Department of Justice's (DOJ) Computer Crimes and Intellectual Property Division to the administration's new National Security Division (NSD), in September 2009 to spearhead the team's cybercrime efforts.

According the NSD's press release, "Mr. Bailey is widely respected within the Justice Department and the Intelligence Community for his knowledge of cyber issues." However, even he admitted he is at a loss for words on the subject. The area suffers from a "limited lexicon," he explained, "we even lack a unified definition of cyberterrorism and that makes discourse on the subject difficult."

The government has failed to convene its various departments to forge a single definition. The FBI alone has published three distinct definitions of cyber-terrorism: "Terrorism that initiates…attack[s] on information" in 1999, to "the use of Cyber tools" in 2000 and "a criminal act perpetrated by the use of computers" in 2004. Other government agencies responsible for responding to cyberattacks, such as the Department of Defense, Federal Emergency Management Agency, National Infrastructure Protection Center, Drug Enforcement Agency, National Homeland Security Agency, and the Department of Justice have each created their own definitions.

Bailey's explanation for the limited and conflicting vocabulary is twofold. First, "the interest in cyber issues only started in the nineties so the terms are still nascent." Secondly, the departments have fragmented the definition because the meaning depends on their differing interests. "Look at the response to Twitter," he observed. "The Department of State lauded its use in Iran, while other departments heavily criticized it."

Unlike Bailey, Kim Taipale, founder and executive director for the Stilwell Center for Advanced Studies in Science and Technology Policy believes "cyberterrorism, whatever it is, is a useless term." Taipale believes that, "terrorists will use any strategic tool they can" so "cyber" terrorism is no more important then other forms. Rather the problem is that there is no "unified legal regime," creating a "gap between law-makers and authorities," he stated. "Whether the military or police should respond, whether it is domestic or foreign is not fully determined," said Taipale. These separate entities are "incompatible and inconsistent, making us more vulnerable to terrorism."

Taipale explained that having such a fragmented legal structure means that we are "not equipped to deal with an array of a whole host of new problems" that cyber issues present. And this is truly

troublesome because the line between “safe society and chaos is a thin one,” said Taipale, “We are in line for some serious cyber-Katrinas that we are not ready to deal with.”

Like Bailey, however, Taipale believes that the “obsolete security infrastructure” exists because different entities have differing concerns. After cyber-threats were made to Slobodan Milosevic’s bank accounts during the 1999 Kosovo crisis, for example, the cyberterrorism discussion was raised in the U.N., and although Russia expressed interest in the problem, the U.S. stalled the discussion. “What is and isn’t permissible was never decided because of the U.S.’ interest in its own international liability,” said Taipale. “Now there are no rules,” he continued. “Now we are reaping the problems.”

Taipale’s fear that the line between safe society and chaos is fragile is compounded by the problem of trust, highlighted by Dr. Andrew Colarik, an information security consultant. Colarik stressed the term’s etymology, saying that “there is no cyberterrorism without terrorism.” In essence, the goal of terrorism is to cause severe disruption through widespread fear in society, meaning “our dependency on digital material,” is the problem, he said. “The majority of our currency is not paper, it’s digital. And like money, if we lose confidence in the underlying system, we will have insolvency.” Colarik argues that we should limit the amount of information we store digitally.

Taipale echoed the doomsday concern, “the U.S. is a real target because of our dependency on the online system.” These attacks are about “exploitation.” “Non-peer” countries don’t depend on the digital system and so they have an opportunity to attack without the risk of suffering from similar counterattacks.

But Bailey believes the problems Taipale and Colarik raise cannot be solved without some basic agreement over terminology. “These are conversations that cannot take place because there is no common language to discuss this,” he said. He suggests as a first step “that we as a government have to consider what we think about these issues first.” The hesitation is that “whatever you decide you have to live with.” While it is possible that trying to divine a definition of cyberterrorism is a fools’ errand, “it is a way of achieving an end.”