7-22-2010

Susan Brenner's Latest Book Examines Criminal

University of Dayton, Ohio (url: http://www.udayton.edu/index.php)

Susan Brenner's Latest Book Examines Criminal Cyberthreats

07.22.2010 | Law, Faculty

Professor Susan Brenner describes her area of research, the topic of cybercrime and cyberterrorism, as "the intersection of good and bad in a context in which none of the traditional assumptions and none of the traditional constraints apply." For instance, in a cybercrime, there is no crime scene, in the traditional sense. The victim can be anyone from a government agency to a multinational corporation to an unsuspecting relative. And the perpetrator can be located almost anywhere in the world. Brenner examines these challenges in her latest book, *Cybercrime: Criminal Threats from Cyberspace (url: http://amzn.com/0313365466)* , published by Praeger.

Geared toward a general audience, *Cybercrime* is the culmination of Brenner's work over the last 13 years, beginning in 1997 when she taught her first cybercrime seminar at Dayton Law. Over the next several years, she became involved in efforts to combat cybercrimes that were undertaken by various U.S. and foreign government agencies. After 9/11, she became interested in cyberterrorism, which was being discussed as a real threat.

"I began to realize how the three traditional threat categories, war, crime and terrorism, morph and merge into each other when they're carried out via cyberspace. I also realized they take on new forms," said Brenner, the NCR professor of law and technology who also writes the blog CYB3BERCRIM3 (url: http://cyb3rcrim3.blogspot.com/) .

Brenner's research has examined how civilians, as well as governments, can wage war in cyberspace, and how cyberwar is likely to differ from traditional warfare. Last year, Oxford University Press published her book *Cyberthreats: The Emerging Fault Lines of the Nation State*, which explored how cyberspace can be used not only to commit crimes and terrorism, but to carry out warfare. *Cyberthreats* examined how governments, especially the U.S. government, deal with these rapidly emerging, still evolving threats.

With her latest book, *Cybercrime*, Brenner focused on the intersection of computer technology and crime, and how criminals use computer technology, particularly the Internet, to commit crimes.

As Brenner explains in the book, cybercrimes fall into two categories: target crimes, which are crimes that are directed at computers and computer systems, like spreading malware and gaining unauthorized access to computer systems; and tool cybercrimes, which consist of traditional crimes like theft, embezzlement, stalking and extortion but are committed through the use of computer technology.

One example of cybercrime that Brenner cites involved a group, appearing to be operating from Ukraine, that stole the login credentials of the county treasurer of a small Kentucky county and used them to wire to outside the United States funds totaling $415,000 from the county's bank account.

This case shows the challenges law enforcement officials face when investigating such crimes. If the crime had occurred in the physical world, the investigators would have examined the crime scene, discovered clues and interviewed witnesses.

However, the bank theft didn't take place in the physical world. It was committed in the virtual world, in what Brenner called a "nebulous crime scene." Computer forensics experts analyzed where the money had gone and tried to figure out who was responsible by tracing emails and other signals sent to the bank and back to their source.

"But it's often difficult to tell where something really came from because messages and other traffic can be routed through various servers," Brenner said. "Maybe the Kentucky theft was carried out by people in Ukraine . . . or maybe they were in Russia or in Peoria. It takes a great deal of time and effort to try to identify the perpetrators, and if you succeed, you still have to get them."

It's been almost a year and no one has been identified and arrested for the crime, and Brenner assumes no one ever will be caught. "What makes cybercrime, like this theft, so appealing to criminals is that their chances of being apprehended and punished are nil," Brenner said.

"If you can make nearly half a million dollars by expending not that much effort and without running any major risk of being injured or caught," she said, "you might just decide to do something like this, especially if the victim is halfway around the world and in a country you think is too rich to miss the money."

This leads one to ask why average citizens should care about the threat of cybercrime. As Brenner points out, citizens can fall victim to these kinds of threats, including identity theft. "Stalking, harassment and threats have exploded online, and the victims usually have little recourse," she said.

Citizens also should care because their own computers can be used in cybercrimes. Cybercriminals will attack PCs with malware that turns the machines into "zombies," which become soldiers in vast bot (as in "robot") armies of hundreds of thousands (or even millions) of computers. The most common tactic is to use the bot army to shut down an online casino or other online business, then demand money from the company to halt the attack. "The businesses almost always pay, because if they don't they'll lose a great deal of money," Brenner said.

Bot armies of zombie computers have also been used to launch attacks on governments and government systems, she said.

Brenner argues that new ways to combat cybercrime must be developed because, as she said, "we're clearly losing this battle."

One solution is to create a global "Cybercrime Police Force," but Brenner said that "isn't going to happen now or in the foreseeable future, and I doubt many of us would want it to happen."

Brenner advocates for placing more emphasis on prevention of cybercrime. "We have to treat every computer that's linked to the Internet as an open border and do whatever we can to secure that border," she said. "We need to harden our systems to make it as difficult as possible for cybercriminals to penetrate them. We also need to become more sophisticated and less gullible in our dealings with other people online."

So don't send money to a stranger in Romania or to a Nigerian prince. "We all need to become more sophisticated about what's out there," she said, "and what we need to do to avoid becoming victims."

For more information, contact Bob Mihalek, communications specialist at the University of Dayton School of Law, at 937-229-4683 or bob.mihalek@udayton.edu.