1-13-2009

Digital Warriors

Follow this and additional works at: https://ecommons.udayton.edu/news_rls

Recommended Citation
https://ecommons.udayton.edu/news_rls/1613

This News Article is brought to you for free and open access by the Marketing and Communications at eCommons. It has been accepted for inclusion in News Releases by an authorized administrator of eCommons. For more information, please contact frice1@udayton.edu, mshlangen1@udayton.edu.
Digital Warriors

01.13.2009 | Faculty

Susan Brenner doesn't fret about the lone hacker creating a little havoc.

In the post-9/11 world, she worries about nontraditional warfare waged by terrorists using computers as weapons. Brenner, who's conducted cybercrimes training for the U.S. Secret Service and spoken at numerous national and international conferences, predicts cyberspace will become the new battlefield in her newly published book, Cyberthreats: The Emerging Fault Lines of the Nation State (Oxford University Press).

"At some point, we'll see terrorists begin to use cybercrime for their own purposes," said Brenner, NCR professor of law and technology at the University of Dayton and an internationally renowned, prolific scholar in the emerging field.

"With cyberthreats, it is difficult for the attacked to know the identity of the attacker or to determine the nature of the attack — whether war or crime or terrorism. If we don’t know who is attacking, how do we counterattack? If we don’t know whether the attack is a crime or an act of war, we don’t know whether to use the police or the military," she said, noting that the enemy is often invisible and that geography becomes irrelevant.

Pointing to her laptop sitting on her office desk, she added, "That laptop sitting there is a border. It can be exploited." Brenner doesn't go as far as to liken cyberwarfare to Pearl Harbor, but believes the threat is pervasive and a cause for genuine concern. "It wouldn't be hard," she said, "to destabilize smaller countries."

Sound far-fetched? Brenner cites a 2007 two-week digital attack on the country of Estonia, initially believed to originate in Russia, as evidence of the kind of attacks that can shut down government sites and financial institutions and knock out electricity. She believes the U.S. needs to develop a new approach for dealing with cyberthreats and protecting cyberspace.

Her suggestions for a new model?

- Integrate the efforts of the military and law enforcement by collecting and sharing timely information about actual or suspected attacks. Two organizations — U.S. Secret Service's Electronic Crimes Task Forces and the FBI's InfraGard program — already do this, she noted, but more needs to be done to create greater cooperation.
- Involve civilians in the effort. Encourage whistleblowing by citizens to alleviate the underreporting of cybercrime. Encourage victims to report cyberattacks by offering them assurance the information would not be used to initiate criminal proceedings against the perpetrator unless they agreed.
- Create a new federal agency, Cyber Security Agency, to respond to cyberthreats.

The time for greater action is now, in part because the cost of cybercrime is skyrocketing.

"In 2004, the Federal Bureau of Investigation estimated that cybercrime cost U.S. citizens about $400 billion, and in July 2007 FBI Director Robert Mueller said he believes only about one-third of cybercrime in the U.S. is actually reported to the FBI," Brenner said. "I have heard cybercrime estimates are much, much higher than the figure cited for 2004. ...It will continue to increase until governments begin to create realistic disincentives for cybercriminals."

The "cyber-vandals" are not at the gate, and "we are not the Roman Empire in the early fifth century A.D.," but Brenner is sounding the alarm with her book. "I may be wrong, but I suspect the challenges emerging in this area are analogous to pre-shocks that signal an impending earthquake," she said.

Brenner is a member of the American Academy of Forensic Sciences, American Bar Association’s International Cybercrime Project and the U.S. Department of Justice’s National Forensic Science Technology Center Digital Evidence Project. She has served on the National District Attorneys Association’s Committee on Cybercrimes and two Department of Justice digital evidence working groups. She addressed cyberterrorism at the NATO Advanced Research Workshop on cyberterrorism. Her cybercrimes Web site, law.udayton.edu/cybercrimes, was featured on "NBC Nightly News" and she's often quoted by national media about cyberlaw issues.

Susan Brenner at 937-229-2929 or Susan.Brenner@notes.udayton.edu.