2-26-2010

Cybercrime: Criminal Threats from Cyberspace

Susan W. Brenner
University of Dayton, susanwbrenner@yahoo.com

It's done. Can it be stopped?
Can the law pull the plug on cybercrime?

GETTING AWAY WITH

Maybe. Maybe not.

BY THOMAS M. COLUMBUS

Bank robbers used to be famous: Bonnie and Clyde, Willie Sutton, John Dillinger. … They were fodder for headlines and the inspiration for movies.

Today, cybercriminals prefer to loot your bank account anonymously — on a scale undreamed of by the gun-toting gangsters of yesteryear.

Bank robbers and cybercriminals do have in common a love of technological improvements. In the 1930s, before the expansion of federal law enforcement, one could rob a bank in one state and simply drive into the next to elude arrest. Clyde Barrow wrote to Henry Ford thanking him for his automobiles that made eluding police so easy.

Today — as students learn in the Cybersecurity and National Security Law class of Susan Brenner, Samuel A. McCray Chair in Law — cybercriminals continue to use technology to stay a step (or two) ahead of the law.

"Until this class," Cristina Frankian '14 said, "I didn't realize what an issue cybersecurity is. I didn't realize how complicated it is."

That complexity — technological, geographical and legal — presents the legal system, corporations and private citizens a problem that must be confronted, whether through changes in law, enhanced law enforcement or better defenses on the part of potential victims.

Cybercrime seems almost to have been born by accident. Early in the computer age, hacking was like a game. Brenner, in her 2010 book *Cybercrime: Criminal Threats from Cyberspace,* wrote of MIT in the 1970s when one's computer might flash "Give me a cookie," raising fears of lost work. But typing "cookie" would yield a thank you; and not doing anything, "I didn't want a cookie anyway."

No harm, no foul?

As computers became linked through larger networks and through the explosion of personal computers, hacking became more widespread. And hackers morphed into two groups: brilliant programmers and computer criminals. By the end of the 1990s, the problem was serious. On May 4, 2000, computers around the world received an email with the subject line ILOVEYOU and an attachment LOVE-LETTER-FOR-YOU.TXT. Once it was opened, Brenner said, it emailed itself to everyone in that person's address book. And the process repeated and repeated and repeated. The so-called Love Bug destroyed files as it infected 45 million computers in at least 20 countries and caused $8 billion to 10 billion in damage.

Right, **Susan Brenner** *is framed behind a bank of computers in the main campus data center.*

The bug was traced to the Philippines, but no one was convicted of a crime. In 2000, the Philippines had no law against creating and spreading a computer virus.

Soon, the original creators of such malware were joined by others who had as their motive not just destruction but substantial profit. The malware business produces an estimated annual income of more than $100 billion. And it's generally a legal business. Laws prohibit the use of malware but not its creation. Its use, however, is often not reported. For example, if one is running an online casino that could lose millions if its servers were shut down by an attack, one could see wisdom in paying $2,000 a month for "protection."

Part of the difficulty in arresting and prosecuting perpetrators of cybercrime is analogous to those state boundaries that helped bank robbers of the past motor across state lines. Cybercrime is relatively new; quickly changing technology gives criminals new tools and opportunities. Law, however, changes slowly. And it is not a simple thing. The United States alone has 52 sets of laws (the states, the federal government, the District of Columbia).

And, Frankian said, "just look at the Homeland Security site, how many agencies are working on cybersecurity. That creates an overlap of work and a lack of communication. It's inefficient."

And a hacker can be anywhere on earth. And Earth

CYBERCRIME

has 193 countries. Maybe. The United Nations does have 193 members. The U.S. Department of State recognizes 195 nations. FIFA, the governing body of soccer, has 209 national associations. Disagreements about sovereignty, jurisdiction and what constitutes crime are commonplace — making prosecuting attacks on computers difficult.

Computers don't make just good targets for crimes; they are also very useful tools

Will Cristina Frankian '14, who interned with a federal magistrate, have the tools when she goes into practice to take on cybercriminals?

themselves for committing traditional ones such as fraud, harassment and even murder. Some crimes would seem simple to avoid — don't withdraw your savings when you get an email from Nigeria. But many people do. Victims in the United States have lost hundreds of millions of dollars; the amount is estimated because most victims don't report the crime to police.

Those wishing to stalk or harass others have found computers to be a powerful tool. And one that challenges legal descriptions of certain crimes. For example, two sisters, ages 28 and 16, were churchgoers in an Indiana town. Unknown to them, a man who worked at the church created Facebook pages in their names. He posted their photos, addresses, phone numbers and after-school activities. He used the pages to have virtual sex with men around the world. After two years, the church's pastor — about to move on to a new post — was compiling information for his successor about his congregation.

After the confusion turned into a case, one of the sisters wrote to Brenner — who had blogged about it. The sisters were terrified.

The resolution of the case? Because the accused, Brenner said, "did not direct any of his activity toward either victim, he did not commit the crime of harassment." Under a negotiated deal, he pled guilty to a lesser charge, was sentenced to 30 days and a year's probation while receiving counseling. He had to surrender his computer.

Connecting the substantial damage caused by cybercrime to a perpetrator is often difficult if not impossible. Brenner considered the case of Aaron Caffrey, who lived in England with his parents. A chat room user made anti-American comments against Caffrey's online American girlfriend. An attack was launched from Caffrey's computer upon the computer of the person making the perceived insult.

The attack had a large incidental effect. Just nine days after the terrorist attacks of 9/11, the computer system of the Port of Houston — a system essential for navigating ships in and out of the world's eighth busiest harbor — was shut down by an external computer attack.

Caffrey did not contest that the attack came from his computer. The defense claimed that, although his computer launched the attack, he did not. "Someone" must have installed malicious software that took over the computer without his knowledge and then erased all traces of it. He was acquitted.

Often a crime committed across borders does not even come to trial. "A U.S. arrest warrant," Brenner wrote, "is worthless in any other country, in the same way that a French warrant has no effect in the United States."

There are, she noted, formal devices to obtain evidence from other countries, such as letters rogatory, treaty requests and requests for assistance under executive agreements. Letters rogatory, however, can take years. Requests under a mutual assistance treaty are faster but still can take months or longer. Assistance under executive agreements, which do not have to be approved by Congress, have been used primarily to stem narcotics trafficking; they are unlikely to be used for attacking cybercrime. Informal cooperation is faster although dependent upon networks of individuals willing to aid each other.

Even if evidence is gathered, bringing the accused to trial can be difficult. A country with an extradition treaty with another may be reluctant to give up one of its citizens to be prosecuted for a crime that may not be seen as serious when it occurs somewhere else. And a country without an extradition treaty has no legal obligation.

For an example of how complex a situation can be, Brenner pointed to the Rome Labs case. The Rome Air Force Development Center at Griffiss Air Force Base in New York serves as, in the words of a Senate report, "the Air Force's premier command and control research facility." In the mid-1990s, hackers installed programs on the labs' networks and collected passwords, suggesting that they could access the labs' databases. Four weeks of investigation followed a cybertrail through South Africa, Mexico and European countries before finding in London one of the two perpetrators: a 16-year-old music student. Two more years of work led to the 21-year-old son of a police officer. The 16-year-old, prosecuted in England, pled guilty to 12 counts of violating the Computer Misuse Act. Charges against the other were dropped.

A more recent case illustrates the difficulty when a cybercrime originates in a country with which the U.S. does not have an extradition treaty. Hackers broke into the systems of 40 U.S. companies, including banks, and tried to coerce the companies into hiring them as "security consultants."

One company responded by hiring its

own cybercriminals to counterattack; the counterattack failed as it was deflected into an attack on the other companies. Another company refused to pay the $500,000 "consulting fee." Its website was knocked offline. The company went to the FBI, which suggested drawing out negotiations with the hackers. One of the hackers, in an apparent attempt to land a job, sent his resume. That incautious act helped the FBI trace the source of the attack to Russia, with whom the U.S. does not have an extradition treaty.

Russia ignored requests that it detain the hacker. So, he and a partner were invited to come to the U.S. for a job interview. They did and gladly demonstrated their hacking skills; this allowed the FBI to record their work, gaining access to their Russian server. They were arrested. The two argued their Fourth Amendment rights had been violated since the FBI did not have a search warrant. A federal judge, however, ruled the search took place in Russia, the site of the server, not in the U.S., so the Fourth Amendment did not apply. The two went to jail.

Russia requested that the FBI agent be surrendered for prosecution in Russia. According to Brenner, "the United States has apparently never responded."

What other options did the FBI have? Kidnapping is a legal, though hardly practical, option, Brenner noted. An 1886 Supreme Court ruling, recently upheld, said "the power of a court to try a person for crime is not impaired by the fact that he had been brought within the court's jurisdiction by reason of a 'forcible abduction.'"

Law enforcement has serious problems in its attempts to counter cybercrime. Law and law enforcement evolve. Technology changes faster.

For millennia before the creation of the Metropolitan Police in 19th-century London and its descendants worldwide, policing was the work of either the military or of amateurs. In England over the centuries, a "hue and cry" aroused the citizenry to pursue a criminal. Over time experiments were made with private police forces until in 1829 Sir Robert Peel created the London Metropolitan Police. That model remains today.

But it was created with assumptions that fall apart in cyber reality. It assumes real-world crime, which Brenner pointed out, by being committed in a tangible physical environment, has four characteristics: proximity, scale, physical constraints, and patterns. It's hard to physically attack or physically rob somebody who is halfway around the world. Real-world crime is often on an old-fashioned one-to-one basis. Real-world crime occurs in a specific place; the criminal has to be familiar with it, often has to be there. And much real-world crime is tracked because criminals repeat actions; they have patterns.

Cybercrime is automated. "Perpetrators," Brenner wrote, "can commit thousands of crimes quickly and with little ef-

Privacy, anyone?

The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated …

Then, one might ask, "Why does it seem like everybody on earth can read my email?"

The Fourth Amendment may be the same as it was in the 18th century, but the world is different. So what is the state now of the right of Americans against unreasonable search and seizure?

Susan Brenner, in her book, *Cybercrime: Criminal Threats from Cyberspace*, summarized the history of the application of the Fourth Amendment and looked at issues presented by cyber-reality.

Until the 15th century in England, government searches of private property were, Brenner wrote, almost unknown. In the late 15th century, some guilds were authorized to search private property to enforce their regulations. A century later, the Court of the Star Chamber gained the authority to search and to seize books unlawfully printed. Heretics and political dissenters as well as printers became targets.

In the 18th century, courts became more likely to side with the citizens, and an Englishman's home did become more like a castle. That an exception seemed to be made for citizens residing in the American colonies was a cause of both revolution and the adoption of the Fourth Amendment to the U.S. Constitution. For a century, American courts had little trouble in applying the amendment; it obviously applied to searches of people and places.

In 1876, Congress passed a law to protect people from being defrauded by crooked lotteries using the U.S. mail. A citizen challenged the constitutionality of the law. He lost, but the Supreme Court did hold that sealed mail (as distinct from items such as newspapers) was fully guarded from inspection "as if they were retained by the parties forwarding them in their own domiciles."

Also in 1876, Alexander Graham Bell invented the telephone. Soon police began tapping phones; this was seen — since calls went through an operator — as akin to reading someone's postcard, not opening a sealed letter. By the 1920s, however, operators were replaced by automated systems. Roy Olmstead, a convicted bootlegger, appealed because wiretap evidence was used to convict him. A Supreme Court majority upheld the conviction; the man's home had not been entered.

Justice Louis Brandeis dissented. "He was able to grasp," Brenner wrote, "the significance of the new technology."

Brandeis wrote: "The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may … be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose … the most intimated occurrences of the home. … That places the liberty of every man in the hands of every petty officer."

In 1965 the Supreme Court overturned the Olmstead decision. A 1979 decision, however, ruled that the government could use devices to record phone numbers a person calls and numbers from which calls come to that person. Justice Thurgood Marshall dissented, as does professor Brenner.

Then came email.

It's not like a letter. Unless one encrypts email (and, Brenner notes, few do outside of the military and intelligence communities), email is treated as a postcard. Since the same technology that scans for spam and obscenity can scan for other content, the government, employers and others can have easy access to the content of email. The government would need a court order or subpoena. Employers can generally just rely on employees to click "I agree" on email policies. And the material in the "to" and "from" fields and the data generated as the email is transmitted have no Fourth Amendment protection whatsoever.

The Internet is not one's physical castle. And its legal bulwarks are an evolving field.

fort." And with little regard to boundaries.

With law enforcement response to cybercrime, Frankian said, "there is no time for strategy or analysis. An attack can come from anywhere. And you don't see it coming."

At the same time, "cybercrime has not altered people's inclination," Brenner wrote, "to rape, rob or kill in the real world." Added to the increased quantity of crimes are enforcement difficulties peculiar to cybercrime. The police often aren't involved until well after the crime is committed and the trail has become cold. Evidence is fragile and volatile. And the hesitancy to report cybercrime makes establishing patterns different.

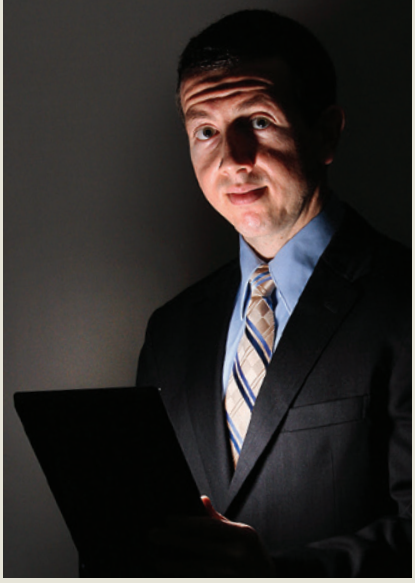
What can be done?

Brenner noted that efforts have been made by several organizations. International studies of cybercrime have been done since the 1980s. The Council of Europe drafted a cybercrime treaty to harmonize national laws. The United Nations passed a resolution. The G8 and other groups of nations have called for consistent laws.

But because of nations' concerns for their sovereignty, it is unlikely they will cede power to a central policing agency. INTERPOL, for example, has a cybercrime initiative but focuses on supporting law enforcement at the national level.

A treaty, the Convention on Cybercrime, was in 2001 presented to countries for ratification. By the time of Brenner's 2010 book, it had been signed by 46 countries and ratified by 20, the United States and 19 European countries. Russia refused to sign it. And many countries aren't just passively opposed; some operate like the island havens for sea-going pirates of the 1600s. Having your nation's banking operations secret may not be something pleasing to other nations — but it can be very profitable.

Awaiting attack



"This is a very complacent country," Susan Brenner said. "Europe is not. They've been attacked, invaded and bombed by neighbors. We've gotten used to being bordered by Mexico and Canada."

And having a big ocean on each side and the world's most powerful air force overhead can also bolster our feeling of security.

Brenner does not worry, however, about the country being physically invaded but about its citizens being the victims of cyberattacks launched by criminals, often from the security of havens in rogue states.

"It's amazing how vulnerable we are," said Aaron Wiener '14 (pictured above), a student this past fall in Susan Brenner's Cybersecurity and National Security Law class. "Security is expensive, and the threat is not perceived."

Even before entering UDSL, however, Wiener began trying to spread awareness of the threat and do something to improve defenses against it.

"Accountants often send unsecured email and faxes," he said, "an identity thief's dream come true."

Wiener, who was a communication major at the University of Illinois, joined forces with friends who were knowledgeable about accounting to found DocPalApp.com, an application that provides accountants a secure way to transmit documents. He hopes that the app having been developed specifically for accountants will give it a market edge over more generic devices.

Whatever method accountants or other business people choose, "we have to say to citizens," Brenner said, "protect yourselves. And a lot of businesses are coming to realize this."

Some solutions offered to combat cybercrime do not focus on the law. Frankian this year did research on cyberdefense. The option of offensive measures ("hacking back"), though illegal, has recently gained momentum and is supported by U.S. companies who have been the victims of destructive and costly cyberattacks.

"Companies work with others," she said, "essentially cybermercenaries who could counterattack. But an 'eye-for-an-eye' could become cyberwar."

That's partly because finding the target can be difficult. The hacker in the Rome Labs case, Brenner pointed out, "routed his attack through a North Korean nuclear facility. Hacking back would have attacked that."

Frankian, in her research this past term, looked at an alternative to counterattack: empowering the government to help companies establish a good defense. She envisions the possibility of an overarching federal agency not only to regulate, she said, but also "to reach out to businesses, financial institutions and utilities to see where they are vulnerable, to see what they need in case of cyberattack."

Such an approach may not be as grand a plan as rewriting laws in some 200 nations or hiring bands of mercenary hackers, but as Brenner wrote, "Encouraging cybercrime prevention is not a particularly exciting strategy, but it would probably make cybercriminals' lives more difficult [and] it could increase the effectiveness of law enforcement efforts." ■

For further reading

Students set up a fake social media account in the name of their assistant principal. They use the account to invite children to communicate with, the children think, the assistant principal. The children are then bombarded with porn.

The assistant principal sues in federal court.

He loses.

After all, the judge noted, even Facebook admitted that nearly 10 percent of its users were "duplicates, false or undesirable."

The assistant principal "can presumably try suing in state court," Susan Brenner wrote in her blog CYB3RCRIM3 (cyb3rcrim3.blogspot.com), where she has analyzed that case and hundreds of others in detail.

Brenner, Samuel A. McCray Chair in Law, has also published several books and journal articles on cybercrime (see www.udayton.edu/directory/law/brenner_susan.php).